IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

JENNIFER CABEZAS *et al*., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MR. COOPER GROUP INC. and NATIONSTAR MORTGAGE LLC d/b/a MR. COOPER,

Defendants.

Case No. 3:23-cv-024530-N

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

1. Plaintiffs Jose Ignacio Garrigo, Izabela Debowcsyk, Joshua Watson, Brett Padalecki, Chris Leptiak, Denver Dale, Emily Burke, Mary Crawford, Kay Pollard, Jonathan Josi, Jeff Price, Mychael Marrone, Katy Ross, Lynette Williams, Karen Lynn Williams, Gary Allen, Larry Siegal, Rohit Burani, Elizabeth Curry, Justin Snider, Linda Hansen, and Deira Robertson (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Defendants Mr. Cooper Group, Inc. and Nationstar Mortgage LLC d/b/a Mr. Cooper (collectively, "Defendants" or "Mr. Cooper"), based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents, as to all other matters.

INTRODUCTION

2. In 2023, Mr. Cooper celebrated as it became "America's largest mortgage loan servicer" with nearly 5 million customers and a loan portfolio of $1 trillion. As part of that

growth, Mr. Cooper swept up a huge cache of customer information. But Mr. Cooper left that information unencrypted and unprotected from data thieves. In late 2023, Mr. Cooper suffered one of the largest data breaches ever recorded, compromising the names, addresses, phone numbers, Social Security numbers, dates of birth and bank account numbers on nearly 15 million current and former customers. After numerous denials and half-truths, Mr. Cooper acknowledged to regulators that the breach was catastrophic. In Mr. Cooper's words: ***"Our forensic review determined that personal information relating to substantially all current and former customers was obtained from our systems during this incident."*** The fallout from Mr. Cooper's failure to protect customer information has been substantial and will be long-lasting. This Consolidated Complaint seeks redress for Mr. Cooper's conduct.

THE PARTIES

Plaintiff Kay Pollard

3. Plaintiff Pollard is and at all relevant times was a citizen of the state of Florida and the United States.

4. Plaintiff Pollard is currently a Mr. Cooper customer and was a customer at the time of the data breach and on October 31, 2023, when she received a notice informing her that she was impacted by the Data Breach.

5. Plaintiff Pollard's mortgage was acquired by Mr. Cooper from Rushmore prior to the Data Breach. In the course of obtaining the mortgage, Plaintiff Pollard was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Pollard reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

6. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Pollard's PII in their system.

7. Plaintiff Pollard received a notification letter from Mr. Cooper on or about December 2023, stating that Plaintiff Pollard's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, phone number, and address.

8. The letter recommended that Plaintiff Pollard take certain actions like monitoring her accounts and remaining vigilant against incidents of identity theft and fraud, to review her account statements, and to monitor her credit reports for suspicious activity. Despite making these recommendations to Plaintiff Pollard and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

9. As a result of the Data Breach, Plaintiff Pollard has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: monitoring her credit card and other financial statements for any signs of fraudulent activity daily after already being the victim of fraudulent credit card charges since the Data Breach, checking her credit report daily after already discovering unauthorized activity appearing on her credit report since the Data Breach, telephone calls to retailers regarding unauthorized charges occurring, telephone calls with Mr. Cooper regarding the Data Breach, researching and verifying the legitimacy of the Data Breach upon receiving a notice, and managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Pollard has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities,

including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

10. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Pollard has already experienced the effects of the dissemination of her PII through the Data Breach. Specifically, as a result of the Data Breach, Plaintiff Pollard has experienced several fraudulent credit card charges, which required her to close those accounts. Plaintiff Pollard has also experienced numerous unauthorized credit report inquiries, which required her to put a freeze on her credit. Each time she attempted to unfreeze her credit, she would be immediately bombarded with unauthorized activity on her credit report, which required her to repeat the process of freezing her credit. Further, Plaintiff Pollard was required to reset automatic billing instructions she had in place tied to accounts that were compromised after the Data Breach.

11. Plaintiff Pollard also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

12. To date, Plaintiff Pollard has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Pollard values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. As a disabled military veteran and single mother of two children currently in college, Plaintiff Pollard has experiences substantial stress and concern over the burden placed upon her by way of fraudulent credit card charges and the need to close accounts and place a freeze on her credit.

13. The fear, anxiety, and stress experienced by Plaintiff Pollard as a result of the

Data Breach has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

14. Had Plaintiff Pollard been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Pollard has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Pollard anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

15. Plaintiff Pollard suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

16. As a result of the Data Breach, Plaintiff Pollard is and will continue to be at increased risk of identity theft and fraud for years to come.

17. Plaintiff Pollard has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from

future breaches.

18. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Pollard's PII on its internal systems. Thus, Plaintiff Pollard has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Katy Ross

19. Plaintiff Ross is and at all relevant times was a citizen of the state of North Carolina and the United States.

20. Plaintiff Ross is currently a Mr. Cooper customer and was a customer at the time of the data breach and when she received a notice informing her that she was impacted by the Data Breach.

21. In the course of obtaining her mortgage, Plaintiff Ross was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Ross reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

22. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Ross' PII in their system.

23. Plaintiff Ross received a notification letter from Mr. Cooper in or around December 2023, stating that Plaintiff Ross' PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, phone number, and address.

24. The letter recommended that Plaintiff Ross take certain actions like monitoring her accounts and remaining vigilant against incidents of identity theft and fraud, to review her

account statements, and to monitor her credit reports for suspicious activity. Despite making these recommendations to Plaintiff Ross and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

25. As a result of the Data Breach, Plaintiff Ross has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: filing a complaint with the North Carolina Attorney General's Office, filing a complaint with the Federal Trade Commission, filing a report with the Federal Bureau of Investigation, monitoring her credit card and other financial statements for any signs of fraudulent activity daily after already being the victim of a $25,000 theft from her Charles Schwab account, checking her credit report daily, needing to freeze her credit, researching and verifying the legitimacy of the Data Breach upon receiving a notice, and managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Ross has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

26. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Ross has already experienced the effects of the dissemination of her PII through the Data Breach. Specifically, as a result of the Data Breach, Plaintiff Ross had $25,000 stolen from her Charles Schwab account by a bad actor in January 2024, which resulted in her contacting law enforcement and filing a report with the Federal Bureau of Investigation.

27. Plaintiff Ross also suffered actual injury in the form of receiving an alert that her

PII was detected on the Dark Web and experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

28. To date, Plaintiff Ross has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Ross values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach. As a disabled military veteran and single mother of two children currently in college, Plaintiff Ross has experienced substantial stress and concern over the burden placed upon her by way of fraudulent credit card charges and the need to close accounts and place a freeze on her credit.

29. The fear, anxiety, and stress experienced by Plaintiff Ross as a result of the Data Breach has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

30. Had Plaintiff Ross been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Ross has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Ross anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

31. Plaintiff Ross suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

32. As a result of the Data Breach, Plaintiff Ross is and will continue to be at increased risk of identity theft and fraud for years to come.

33. Plaintiff Ross has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

34. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Ross' PII on its internal systems. Thus, Plaintiff Ross has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Gary Allen

35. Plaintiff Allen is and at all relevant times was a citizen of the state of New York and the United States.

36. Plaintiff Allen is a former customer of Mr. Cooper.

37. Plaintiff Allen's mortgage changed ownership several times before being acquired by Mr. Cooper. In the course of obtaining the mortgage, Plaintiff Allen was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Allen reasonably expected that his PII would remain safe and not be accessed by

unauthorized third parties.

38. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Allen's PII in their system.

39. Plaintiff Allen received a notification letter from Mr. Cooper dated December 17, 2023, stating that his PII was improperly accessed and obtained by unauthorized third parties, including his name, address, and Social Security number.

40. The letter recommended that Plaintiff Allen take certain actions like monitoring his accounts and remaining vigilant against incidents of identity theft and fraud, to review his account statements, and to monitor his credit reports for suspicious activity. Despite making these recommendations to Plaintiff Allen and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

41. As a result of the Data Breach, Plaintiff Allen has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: monitoring his credit card and other financial statements for any signs of fraudulent activity daily after already being the victim of fraudulent credit card charges since the Data Breach, checking his credit report daily after already discovering unauthorized activity appearing on his credit report since the Data Breach, telephone calls to retailers regarding unauthorized charges occurring, researching and verifying the legitimacy of the Data Breach upon receiving a notice, managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Allen has spent significant time dealing with the Data Breach, valuable time Plaintiff Allen otherwise would have spent on other activities, including but not limited to work and/or recreation. This

time has been lost forever and cannot be recaptured.

42. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Allen has already experienced the effects of the dissemination of his PII through the Data Breach. Specifically, as a result of the Data Breach, Plaintiff Allen has experienced several fraudulent credit card charges made to his accounts, has been notified by Microsoft that a bad actor attempted to access his Microsoft account from an undisclosed location in China, has discovered several attempts to open new accounts in his name, and several unauthorized credit inquiries that appeared on his credit report.

43. Plaintiff Allen also suffered actual injury in the form of experiencing an increase in spam/phishing calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach, and which Plaintiff Allen estimates to be in the number of tens of thousands.

44. To date, Plaintiff Allen has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Allen values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

45. Had Plaintiff Allen been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Allen has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Allen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

46. Plaintiff Allen suffered actual injury from having his PII compromised as a result

of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

47. The Data Breach has caused Plaintiff Allen to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

48. As a result of the Data Breach, Plaintiff Allen is and will continue to be at increased risk of identity theft and fraud for years to come.

49. Plaintiff Allen has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

50. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Allen's PII on its internal systems. Thus, Plaintiff Allen has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Brett Padalecki

51. Plaintiff Padalecki is and at all relevant times was a citizen of the state of Nevada and the United States.

52. Plaintiff Padalecki is currently a Mr. Cooper customer and was a customer at the

time of the data breach, and when he received a notice informing him that he was impacted by the Data Breach.

53. Plaintiff Padalecki's mortgage was originated by another company prior to being acquired by Mr. Cooper. In the course of obtaining the mortgage, Plaintiff Padalecki was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Padalecki reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

54. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Padalecki's PII in their system.

55. Plaintiff Padalecki received a notification letter from Mr. Cooper in December 2023, stating that Plaintiff Padalecki's PII was improperly accessed and obtained by unauthorized third parties, including his name, address, and Social Security number.

56. The letter recommended that Plaintiff Padalecki take certain actions like monitoring his accounts and remaining vigilant against incidents of identity theft and fraud, to review his account statements, and to monitor his credit reports for suspicious activity. Despite making these recommendations to Plaintiff Padalecki and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

57. As a result of the Data Breach, Plaintiff Padalecki has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring

his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Padalecki has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

58. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Padalecki has already experienced the effects of the dissemination of his PII through the Data Breach, having experienced a substantial increase in spam/phishing emails, calls, and texts since the Data Breach.

59. To date, Plaintiff Padalecki has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Padalecki values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

60. Had Plaintiff Padalecki been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Padalecki has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Padalecki anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

61. Plaintiff Padalecki suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate

the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

62. The Data Breach has caused Plaintiff Padalecki to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

63. As a result of the Data Breach, Plaintiff Padalecki is and will continue to be at increased risk of identity theft and fraud for years to come.

64. Plaintiff Padalecki has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

65. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Padalecki's PII on its internal systems. Thus, Plaintiff Padalecki has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Jeff Price

66. Plaintiff Price is and at all relevant times was a citizen of the state of Illinois and the United States.

67. Plaintiff Price is a former customer of Mr. Cooper, who was a Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice

informing him that he was impacted by the Data Breach.

68. In the course of obtaining his mortgage, Plaintiff Price was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Price reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

69. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Price's PII in their system.

70. Plaintiff Price received a notification letter from Mr. Cooper in or around December 2023, stating that his PII was improperly accessed and obtained by unauthorized third parties, including his name, address, and Social Security number.

71. The letter recommended that Plaintiff Price take certain actions like monitoring his accounts and remaining vigilant against incidents of identity theft and fraud, to review his account statements, and to monitor his credit reports for suspicious activity. Despite making these recommendations to Plaintiff Price and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

72. As a result of the Data Breach, Plaintiff Price has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis.

Plaintiff Price has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

73. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Price has already experienced the effects of the dissemination of his PII through the Data Breach, having experienced a substantial increase in spam/phishing emails, calls, and texts since the Data Breach.

74. To date, Plaintiff Price has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Price values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

75. Had Plaintiff Price been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Price has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Price anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

76. Plaintiff Price suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data

Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

77. The Data Breach has caused Plaintiff Price to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

78. As a result of the Data Breach, Plaintiff Price is and will continue to be at increased risk of identity theft and fraud for years to come.

79. Plaintiff Price has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

80. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Price's PII on its internal systems. Thus, Plaintiff Price has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Larry Siegal

81. Plaintiff Siegal is and at all relevant times was a citizen of the state of Illinois and the United States.

82. Plaintiff Siegal is currently a Mr. Cooper customer and was a customer at the time of the data breach and on October 31, 2023, when she received a notice informing her that she was impacted by the Data Breach.

83. Plaintiff Siegal's mortgage was acquired by Mr. Cooper from another company prior to the Data Breach. In the course of obtaining the mortgage, Plaintiff Siegal was required,

directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Siegal reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

84. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff Siegel's PII in their system.

85. Plaintiff Siegel received a notification letter from Mr. Cooper in or around December 2023, stating that Plaintiff Siegel's PII was improperly accessed and obtained by unauthorized third parties, including his name, address, and Social Security number.

86. The letter recommended that Plaintiff Siegel take certain actions like monitoring his accounts and remaining vigilant against incidents of identity theft and fraud, to review his account statements, and to monitor his credit reports for suspicious activity. Despite making these recommendations to Plaintiff Siegal and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

87. As a result of the Data Breach, Plaintiff Siegel has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Siegel has spent significant time dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including but not limited to work and/or

recreation. This time has been lost forever and cannot be recaptured.

88. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Siegel has already experienced the effects of the dissemination of his PII through the Data Breach, having received a notification from Credit Karma that his information was discovered on the Dark Web and having experienced a substantial increase in spam/phishing emails, calls, and texts since the Data Breach.

89. To date, Plaintiff Siegel has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Siegel values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

90. Had Plaintiff Siegel been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Siegel has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Siegel anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach.

91. Plaintiff Siegel suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to

his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

92. The Data Breach has caused Plaintiff Siegel to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

93. As a result of the Data Breach, Plaintiff Siegel is and will continue to be at increased risk of identity theft and fraud for years to come.

94. Plaintiff Siegel has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

95. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Siegel's PII on its internal systems. Thus, Plaintiff Siegel has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Jose Ignacio Garrigo

96. Plaintiff Jose Ignacio Garrigo ("Garrigo") is and at all relevant times was a citizen of the state of Montana and the United States.

97. Plaintiff Garrigo was a Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice informing him that he was impacted by the Data Breach.

98. Plaintiff Garrigo entered into a mortgage transaction with the United Services Automobile Association ("USAA") in September 2022. His mortgage was acquired by Mr.

Cooper shortly thereafter in November 2022. In the course of obtaining the mortgage, Plaintiff Garrigo was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Garrigo reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

99. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

100. Plaintiff Garrigo received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Garrigo's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

101. The letter recommended that Plaintiff Garrigo take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

102. As a result of the Data Breach, Plaintiff Garrigo has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis.

Plaintiff Garrigo has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

103. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Garrigo has already experienced the effects of the dissemination of his PII on the Dark Web. Plaintiff Garrigo experienced a fraudulent charge on his Discover credit card. Plaintiff Garrigo has also seen an increase in spam texts and phone calls since the breach.

104. To date, Plaintiff Garrigo has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Garrigo values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

105. Had Plaintiff Garrigo been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Garrigo has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Garrigo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

106. Plaintiff Garrigo suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the

bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

107. The Data Breach has caused Plaintiff Garrigo to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

108. As a result of the Data Breach, Plaintiff Garrigo is and will continue to be at increased risk of identity theft and fraud for years to come.

109. Plaintiff Garrigo has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

110. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Garrigo's PII on its internal systems. Thus, Plaintiff Garrigo has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Denver Dale

111. Plaintiff Denver Dale ("Dale") is and at all relevant times was a citizen of the state of California and the United States.

112. Plaintiff Dale was a Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice informing him that he was impacted by the Data Breach.

113. Plaintiff Dale's mortgage was acquired by Mr. Cooper in 2014. In the course of obtaining the mortgage, Plaintiff Dale was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Dale reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

114. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

115. Plaintiff Dale received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Dale's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

116. The letter recommended that Plaintiff Dale take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

117. As a result of the Data Breach, Plaintiff Dale has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis.

Plaintiff Dale has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

118. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Dale has already experienced the effects of the dissemination of his PII on the Dark Web. Plaintiff Dale received alerts from Experian that his information is on the Dark Web. Plaintiff Dale has also seen an increase in spam texts and phone calls since the breach.

119. To date, Plaintiff Dale has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Dale values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

120. Had Plaintiff Dale been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Dale has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Dale anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

121. Plaintiff Dale suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

122. The Data Breach has caused Plaintiff Dale to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

123. As a result of the Data Breach, Plaintiff Dale is and will continue to be at increased risk of identity theft and fraud for years to come.

124. Plaintiff Dale has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

125. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Dale's PII on its internal systems. Thus, Plaintiff Dale has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Izabela Debowczyk

126. Plaintiff Izabela Debowczyk ("Debowczyk") is and at all relevant times was a citizen of the state of Illinois and the United States.

127. Plaintiff Debowczyk was a Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

128. Plaintiff Debowczyk's mortgage was acquired by Mr. Cooper in 2019. In the course of obtaining the mortgage, Plaintiff Debowczyk was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Debowczyk reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

129. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

130. On or about January 6, 2024, Plaintiff Debowczyk received a notification letter dated December 20, 2023 from Mr. Cooper stating that Plaintiff Debowczyk's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, date of birth, and full address.

131. Upon information and belief, at the time of the Data Breach, Mr. Cooper possessed additional pieces of Ms. Debowczyk's PII, such as her phone number, email address, home loan billing and payment information, insurance information, and financial status and account information, all of which may have been accessed by unauthorized persons in the Data Breach.

132. The letter recommended that Plaintiff Debowczyk take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr.

Cooper's lack of vigilance and care directly led to the Data Breach.

133. As a result of the Data Breach, Plaintiff Debowczyk has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Debowczyk has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

134. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Debowczyk has already experienced the effects of the dissemination of her PII.

135. Plaintiff Debowczyk has seen an increase in spam texts and phone calls since the breach.

136. To date, Plaintiff Debowczyk has spent multiple hours per week on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Debowczyk values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

137. Had Plaintiff Debowczyk been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII that was stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Debowczyk has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach,

Plaintiff Debowczyk anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

138. Plaintiff Debowczyk suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of the benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

139. The Data Breach has caused Plaintiff Debowczyk to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

140. As a result of the Data Breach, Plaintiff Debowczyk is and will continue to be at increased risk of identity theft and fraud for years to come.

141. Plaintiff Debowczyk has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

142. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Debowczyk's PII on its internal systems. Thus, Plaintiff Debowczyk has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Mary Crawford

143. Plaintiff Mary Crawford ("Crawford") is and at all relevant times was a citizen of the state of Missouri and the United States.

144. Plaintiff Crawford was a Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

145. Plaintiff Crawford's mortgage was acquired by Mr. Cooper in 2014. In the course of obtaining the mortgage, Plaintiff Crawford was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Crawford reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

146. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

147. Plaintiff Crawford received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Crawford's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

148. The letter recommended that Plaintiff Crawford take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its

maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

149. As a result of the Data Breach, Plaintiff Crawford has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Crawford has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

150. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Crawford has already experienced the effects of the Data Breach.

151. At or about the time when the Data Breach was discovered, Plaintiff Crawford was scheduled to close on a house she was purchasing with her husband. In connection with the Data Breach, Mr. Cooper's systems were down, and it was unable to provide a statement of the final payout required on her existing mortgage, which was required to close on the new home. Plaintiff Crawford had to hire counsel to draft documents to address this issue, and she had to place moneys in escrow to account for the uncertainty created by Mr. Cooper's malfunctioning systems.

152. Further, Plaintiff Crawford's husband called Mr. Cooper approximately 20 times a day for three days in an effort to obtain the payout information, to no avail.

153. Also, as a result of the Data Breach, Plaintiff Crawford has also seen an increase

in spam texts and phone calls since the breach, including spam emails.

154. To date, Plaintiff Crawford has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Crawford values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

155. Had Plaintiff Crawford been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Crawford has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Crawford anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

156. Plaintiff Crawford suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

157. The Data Breach has caused Plaintiff Crawford to suffer fear, anxiety, and stress,

which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

158. As a result of the Data Breach, Plaintiff Crawford is and will continue to be at increased risk of identity theft and fraud for years to come.

159. Plaintiff Crawford has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

160. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Crawford's PII on its internal systems. Thus, Plaintiff Crawford has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Linda Hansen

161. Plaintiff Linda Hansen ("Hansen") is and at all relevant times was a citizen of the state of Illinois and the United States.

162. Plaintiff Hansen was a former Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach. Several months prior, Ms. Hansen's mortgage was sold by Mr. Cooper to another company.

163. Plaintiff Hansen's mortgage was acquired by Mr. Cooper in 2014. In the course of obtaining the mortgage, Plaintiff Hansen was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Hansen reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

164. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

165. Plaintiff Hansen received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Hansen's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

166. The letter recommended that Plaintiff Hansen take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

167. As a result of the Data Breach, Plaintiff Hansen has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Hansen has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

168. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Hansen has already experienced the effects of the

dissemination of her PII on the Dark Web. As a result of the Data Breach, bad actors attempted to open four credit cards in her name. These credit cards were branded Chase and Disney. Attempts to obtain fraudulent credit cards using Plaintiff Hansen's name continue to this day, and she has reported some of these to the police.

169. Plaintiff Hansen had to take urgent measures to cancel each of these credit cards upon learning of their existence, spending valuable time and experiencing stress due to the persistent nature of these fraud attempts. She also had to take urgent steps to ensure that her credit score did not suffer from these attempts to perpetrate fraud using PII obtained in the Mr. Cooper breach.

170. Plaintiff Hansen has also seen an increase in spam texts and phone calls since the breach, including spam emails containing pornography, which is offensive to her religious faith.

171. To date, Plaintiff Hansen has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Hansen values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

172. Had Plaintiff Hansen been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Hansen has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Hansen anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

173. Plaintiff Hansen suffered actual injury from having her PII compromised as a

result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

174. The Data Breach has caused Plaintiff Hansen to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

175. As a result of the Data Breach, Plaintiff Hansen is and will continue to be at increased risk of identity theft and fraud for years to come.

176. Plaintiff Hansen has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

177. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Hansen's PII on its internal systems. Thus, Plaintiff Hansen has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Karen Lynn Williams

178. Plaintiff Karen Lynn Williams ("Williams") is and at all relevant times was a citizen of the state of California and the United States.

179. Plaintiff Williams was a Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

180. Plaintiff Williams became a client of Mr. Cooper in 2018, following a refinancing of her mortgage. In the course of obtaining the mortgage, Plaintiff Williams was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Williams reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

181. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

182. Plaintiff Williams received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Williams's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

183. The letter recommended that Plaintiff Williams take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

184. As a result of the Data Breach, Plaintiff Williams has and will continue to take

reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Williams has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. Ther time has been lost forever and cannot be recaptured.

185. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Williams has already experienced the effects of the dissemination of her PII on the Dark Web.

186. In mid-2024, Plaintiff Williams was notified by her financial institution that both her debit and credit cards had fraudulent transactions. She had to cancel the existing debit and credit cards and obtain new ones. She had to reset all of the automatic billing which utilized existing bank cards. In at least one instance before she was notified of the fraudulent transaction, but after her financial institution had apparently detected fraudulent transactions as a result of the Data Breach, her card was declined in a store, leading to embarrassment.

187. To date, Plaintiff Williams has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Williams values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

188. Had Plaintiff Williams been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized

parties, Plaintiff Williams has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Williams anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

189. Plaintiff Williams suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

190. The Data Breach has caused Plaintiff Williams to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

191. As a result of the Data Breach, Plaintiff Williams is and will continue to be at increased risk of identity theft and fraud for years to come.

192. Plaintiff Williams has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

193. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff

Williams's PII on its internal systems. Thus, Plaintiff Williams has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Emily Burke

194. Plaintiff Emily Burke ("Burke") is and at all relevant times was a citizen of the state of Alabama and the United States.

195. Plaintiff Burke was a Mr. Cooper former customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

196. Plaintiff Burke's mortgage was acquired by Mr. Cooper in December 2019 and serviced her mortgage until March 2020. In the course of obtaining the mortgage, Plaintiff Burke was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Burke reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

197. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

198. Plaintiff Burke received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Burke's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

199. The letter recommended that Plaintiff Burke take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper

itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

200. As a result of the Data Breach, Plaintiff Burke has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Burke has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

201. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Burke has already experienced the effects of the dissemination of her PII on the Dark Web. As a result of the Data Breach, bad actors attempted to open eleven (11) credit cards in her name, including Mastercard credit cards co-branded with Ulta Rewards Beauty, Barclays, Carters, Victoria Secret, Macy's and other brands. Plaintiff Burke had to take urgent measures to cancel each of these credit cards upon learning of their existence, spending valuable time and experiencing stress due to the persistent nature of these fraud attempts. She also had to take urgent steps to ensure that her credit score did not suffer from these attempts to perpetrate fraud using PII obtained in the Mr. Cooper breach.

202. In addition, bad actors attempted to purchase two iPhones and add a phone line using the fraudulent credit cards.

203. Finally, Plaintiff Burke received a visa debit card, at her mailing address, but with

another person's name on it. She had to take steps to notify Visa and cancel the card.

204. Plaintiff Burke has also seen an increase in spam texts and phone calls since the breach.

205. To date, Plaintiff Burke has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Burke values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

206. Had Plaintiff Burke been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Burke has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Burke anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

207. Plaintiff Burke suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and

adequate measures to protect the PII.

208. The Data Breach has caused Plaintiff Burke to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

209. As a result of the Data Breach, Plaintiff Burke is and will continue to be at increased risk of identity theft and fraud for years to come.

210. Plaintiff Burke has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

211. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Burke's PII on its internal systems. Thus, Plaintiff Burke has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Deira Robertson

212. Plaintiff Deira Robertson ("Robertson") is and at all relevant times was a citizen of the state of Texas and the United States.

213. Plaintiff Robertson was a Mr. Cooper customer at the time of the data breach and in November 2023 when she received a notice informing her that she was impacted by the Data Breach.

214. Plaintiff Robertson's mortgage was acquired by Mr. Cooper in 2023. In the course of obtaining the mortgage, Plaintiff Robertson was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Robertson reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

215. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

216. Plaintiff Robertson received a notification letter from Mr. Cooper on or about December 19, 2023 stating that Plaintiff Robertson's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

217. The letter recommended that Plaintiff Robertson take certain actions like monitoring her accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

218. As a result of the Data Breach, Plaintiff Robertson has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Robertson has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

219. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Robertson has already experienced the effects of

the dissemination of her PII on the Dark Web. As a result of the Data Breach, Plaintiff Robertson received fraud alerts from Experian that someone had tried to impersonate her in order to obtain credit.

220. Further, Plaintiff Robertson received at least four notifications of dark web activity in the relevant time period, from Chase (twice), Capital One, and Google. These alerts indicated that her information was found on the dark web.

221. Plaintiff Robertson has also seen an increase in spam texts and phone calls since the breach, including spam emails.

222. To date, Plaintiff Robertson has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Robertson values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

223. Had Plaintiff Robertson been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided her PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Robertson has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Robertson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

224. Plaintiff Robertson suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the

bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

225. The Data Breach has caused Plaintiff Robertson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

226. As a result of the Data Breach, Plaintiff Robertson is and will continue to be at increased risk of identity theft and fraud for years to come.

227. Plaintiff Robertson has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

228. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Robertson's PII on its internal systems. Thus, Plaintiff Robertson has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Justin Snider

229. Plaintiff Justin Snider is and at all relevant times was a citizen of the state of Georgia and the United States.

230. Plaintiff Snider was a former Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice informing him that he was impacted by the Data Breach.

231. Plaintiff Snider ceased being a customer of Mr. Cooper in November 2021. In the course of obtaining the mortgage, Plaintiff Snider was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Snider reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

232. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

233. Plaintiff Snider received a notification letter from Mr. Cooper on or about December 23, 2023 stating that Plaintiff Snider's PII was improperly accessed and obtained in October 2023 by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

234. The letter recommended that Plaintiff Snider take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

235. As a result of the Data Breach, Plaintiff Snider has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his

credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Snider has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

236. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Snider has already been notified by his credit monitoring service that his PII has been disseminated on the Dark Web. As a result of the Data Breach, a bad actor has repeatedly attempted to gain access to Plaintiff Snider's bank and PayPal accounts. Plaintiff Snider has also seen an increase in spam texts, emails, and phone calls since the breach.

237. To date, Plaintiff Snider has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Snider values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

238. Had Plaintiff Snider been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Snider has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Snider anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

239. Plaintiff Snider suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii)

lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

240. The Data Breach has caused Plaintiff Snider to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

241. As a result of the Data Breach, Plaintiff Snider is and will continue to be at increased risk of identity theft and fraud for years to come.

242. Plaintiff Snider has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

243. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Snider's PII on its internal systems. Thus, Plaintiff Snider has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Chris Lepitak

244. Plaintiff Chris Lepitak is and at all relevant times was a citizen of the state of California and the United States.

245. Plaintiff Lepitak was a Mr. Cooper customer at the time of the data breach and in

December 2023 when he received a notice informing him that he was impacted by the Data Breach.

246. Plaintiff Lepitak's mortgage was acquired by Mr. Cooper in February 2023. In the course of obtaining the mortgage, Plaintiff Lepitak was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Lepitak reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

247. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

248. Plaintiff Lepitak received a notification letter from Mr. Cooper in or about December 2023 stating that Plaintiff Lepitak's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

249. The letter recommended that Plaintiff Lepitak take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

250. As a result of the Data Breach, Plaintiff Lepitak has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to:

researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Lepitak has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

251. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Lepitak has already experienced the effects of the dissemination of his PII on the Dark Web. As a result of the Data Breach, a bad actor pulled Plaintiff Lepitak's credit report, the report reflected an inquiry from Mr. Cooper, however during Plaintiff Lepitak's discussions with Mr. Cooper, they deny that the inquiry was from them. This has resulted in a drop in Plaintiff Lepitak's credit score. Additionally, a bad actor gained access to Plaintiff Lepitak's credit card and incurred fraudulent charges, forcing him to close the account. Plaintiff Lepitak has also seen an increase in spam texts and phone calls since the breach.

252. To date, Plaintiff Lepitak has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Lepitak values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

253. Had Plaintiff Lepitak been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Lepitak has already suffered injury and remains at a substantial and imminent

risk of future harm. As a result of the Data Breach, Plaintiff Lepitak anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

254. Plaintiff Lepitak suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

255. The Data Breach has caused Plaintiff Lepitak to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

256. As a result of the Data Breach, Plaintiff Lepitak is and will continue to be at increased risk of identity theft and fraud for years to come.

257. Plaintiff Lepitak has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

258. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Lepitak's PII on its internal systems. Thus, Plaintiff Lepitak has a continuing interest in ensuring

that the PII is protected and safeguarded from future breaches.

Plaintiff Rohit Burani

259. Plaintiff Rohit Burani is and at all relevant times lived in the state of Texas and the United States.

260. Plaintiff Burani was not a Mr. Cooper customer at the time of the data breach or in March 2024 when he received a notice informing him that he was impacted by the Data Breach.

261. Plaintiff Burani's mortgage was serviced by Mr. Cooper from August 2019 until August 2021. In the course of obtaining the mortgage, Plaintiff Burani was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Burani reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

262. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system despite Plaintiff Burani no longer being a customer of Mr. Cooper.

263. Plaintiff Burani received a notification letter from Mr. Cooper in or about March 2024 stating that Plaintiff Burani's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

264. The letter recommended that Plaintiff Burani take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper

itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

265. As a result of the Data Breach, Plaintiff Burani has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Burani has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

266. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Burani has already experienced the effects of the dissemination of his PII on the Dark Web. As a result of the Data Breach, a bad actor gained access to Plaintiff Burani's financial account, forcing him to close the account. Plaintiff Burani has also seen an increase in spam texts, emails, and phone calls since the breach.

267. To date, Plaintiff Burani has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Burani values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

268. Had Plaintiff Burani been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized

parties, Plaintiff Burani has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Burani anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

269. Plaintiff Burani suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

270. The Data Breach has caused Plaintiff Burani to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

271. As a result of the Data Breach, Plaintiff Burani is and will continue to be at increased risk of identity theft and fraud for years to come.

272. Plaintiff Burani has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

273. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff

Burani's PII on its internal systems. Thus, Plaintiff Burani has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Mychael Marrone

274. Plaintiff Mychael Marrone is and at all relevant times was a citizen of the state of Minnesota and the United States.

275. Plaintiff Marrone was not a Mr. Cooper customer at the time of the data breach or when he received a notice informing him that he was impacted by the Data Breach.

276. Plaintiff Marrone's mortgage was acquired by Mr. Cooper in June 2024. In the course of obtaining the mortgage, Plaintiff Marrone was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Marrone reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

277. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

278. Plaintiff Marrone received a notification letter from Mr. Cooper on or about January 15, 2024 stating that Plaintiff Marrone's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

279. The letter recommended that Plaintiff Marrone take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr.

Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

280. As a result of the Data Breach, Plaintiff Marrone has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Marrone has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

281. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Marrone has already experienced the effects of the dissemination of his PII on the Dark Web. As a result of the Data Breach, a bad actor has attempted to open a bank account in his name, requiring him to spend time and effort to close the account. In addition, Plaintiff Marrone's credit score dropped as a result of bad actors submitting loan applications in his name through various companies. Plaintiff Marrone has also seen an increase in spam texts and phone calls since the breach.

282. To date, Plaintiff Marrone has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Marrone values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

283. Had Plaintiff Marrone been informed of Mr. Cooper's insufficient data security

measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Marrone has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Marrone anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

284. Plaintiff Marrone suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

285. The Data Breach has caused Plaintiff Marrone to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

286. As a result of the Data Breach, Plaintiff Marrone is and will continue to be at increased risk of identity theft and fraud for years to come.

287. Plaintiff Marrone has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from

future breaches.

288. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Marrone's PII on its internal systems. Thus, Plaintiff Marrone has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Lynette Williams

289. Plaintiff Lynette Williams is and at all relevant times was a citizen of the state of Louisiana and the United States.

290. Plaintiff Williams was a Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

291. Plaintiff Williams's mortgage was acquired by Mr. Cooper in 2022. In the course of obtaining the mortgage, Plaintiff Williams was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Williams reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

292. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

293. Plaintiff Williams received a notification letter from Mr. Cooper in or about December 2023 stating that Plaintiff Williams' PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email address, date of birth, and full address.

294. The letter recommended that Plaintiff Williams take certain actions like

monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

295. As a result of the Data Breach, Plaintiff Williams has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Williams has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

296. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Williams has already experienced the effects of the dissemination of her PII on the Dark Web. As a result of the Data Breach, a bad actor gained access to Plaintiff Williams' bank account, forcing her to close the account. In addition, Plaintiff Williams experienced troubling and unusual activity on her credit report after the breach. Plaintiff Williams has also seen an increase in spam texts and phone calls since the breach.

297. To date, Plaintiff Williams has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Williams values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting

from the Data Breach.

298. Had Plaintiff Williams been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Williams has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Williams anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

299. Plaintiff Williams suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

300. The Data Breach has caused Plaintiff Williams to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

301. As a result of the Data Breach, Plaintiff Williams is and will continue to be at increased risk of identity theft and fraud for years to come.

302. Plaintiff Williams has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

303. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Williams's PII on its internal systems. Thus, Plaintiff Williams has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Joshua Watson

304. Plaintiff Joshua Watson is and at all relevant times was a citizen of the state of Missouri and the United States.

305. Plaintiff Watson was a Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice informing him that he was impacted by the Data Breach.

306. Plaintiff Watson became a Mr. Cooper customer in 2016. In the course of obtaining the mortgage, Plaintiff Watson was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Watson reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

307. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

308. Plaintiff Watson received a notification letter from Mr. Cooper in or about December 2023 stating that Plaintiff Watson's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

309. The letter recommended that Plaintiff Watson take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

310. As a result of the Data Breach, Plaintiff Watson has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Watson has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

311. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Watson has already experienced the effects of the dissemination of his PII on the Dark Web. He has received multiple notices from his identity monitoring service that his PII has been found on the Dark Web. Plaintiff Watson has also seen an increase in spam texts, emails, and phone calls since the breach.

312. To date, Plaintiff Watson has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Watson values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from

the Data Breach.

313. Had Plaintiff Watson been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Watson has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Watson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

314. Plaintiff Watson suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

315. The Data Breach has caused Plaintiff Watson to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

316. As a result of the Data Breach, Plaintiff Watson is and will continue to be at increased risk of identity theft and fraud for years to come.

317. Plaintiff Watson has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches. a

318. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Watson's PII on its internal systems. Thus, Plaintiff Watson has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Jonathan Josi

319. Plaintiff Jonathan Josi is and at all relevant times was a citizen of the state of Washington and the United States.

320. Plaintiff Josi was a Mr. Cooper customer at the time of the data breach and in December 2023 when he received a notice informing him that he was impacted by the Data Breach.

321. Plaintiff Josi's mortgage was acquired by Mr. Cooper in 2023 In the course of obtaining the mortgage, Plaintiff Josi was required, directly or indirectly, to provide his PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with his PII, Plaintiff Josi reasonably expected that his PII would remain safe and not be accessed by unauthorized third parties.

322. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

323. Plaintiff Josi received a notification letter from Mr. Cooper in or about December 2023 stating that Plaintiff Josi's PII was improperly accessed and obtained by unauthorized third parties, including his full name, Social Security number, phone number, email address, date of birth, and full address.

324. The letter recommended that Plaintiff Josi take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

325. As a result of the Data Breach, Plaintiff Josi has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring his credit card and other financial statements for any signs of fraudulent activity; monitoring his credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Josi has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

326. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Josi has already experienced the effects of the dissemination of his PII on the Dark Web. As a result of the Data Breach, a bad actor gained access to Plaintiff Josi's bank account, forcing him to close the account. Plaintiff Josi has also seen an increase in spam texts and phone calls since the breach.

327. To date, Plaintiff Josi has spent multiple hours on efforts to react to and protect himself from harm resulting from the Data Breach. Plaintiff Josi values his privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the

Data Breach.

328. Had Plaintiff Josi been informed of Mr. Cooper's insufficient data security measures to protect his PII, he would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Josi has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Josi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

329. Plaintiff Josi suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

330. The Data Breach has caused Plaintiff Josi to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

331. As a result of the Data Breach, Plaintiff Josi is and will continue to be at increased risk of identity theft and fraud for years to come.

332. Plaintiff Josi has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

333. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Josi's PII on its internal systems. Thus, Plaintiff Josi has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Plaintiff Elizabeth Curry

334. Plaintiff Elizabeth Curry is and at all relevant times was a citizen of the state of Colorado and the United States.

335. Plaintiff Curry was a Mr. Cooper customer at the time of the data breach and in December 2023 when she received a notice informing her that she was impacted by the Data Breach.

336. Plaintiff Curry's mortgage was acquired by Mr. Cooper in 2021 or 2022. In the course of obtaining the mortgage, Plaintiff Curry was required, directly or indirectly, to provide her PII, including name, Social Security number, date of birth, address, and highly sensitive bank account information. When providing and entrusting Mr. Cooper with her PII, Plaintiff Curry reasonably expected that her PII would remain safe and not be accessed by unauthorized third parties.

337. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiff's PII in their system.

338. Plaintiff Curry received a notification letter from Mr. Cooper in or about December 2023 stating that Plaintiff Curry's PII was improperly accessed and obtained by unauthorized third parties, including her full name, Social Security number, phone number, email

address, date of birth, and full address.

339. The letter recommended that Plaintiff Curry take certain actions like monitoring his accounts and "remain[ing] vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity." Despite making these recommendations to Plaintiff and the other victims of the Data Breach, Mr. Cooper itself was not vigilant in protecting against the foreseeable risks associated with its maintenance and storage of the highly sensitive information with which it was entrusted. Mr. Cooper's lack of vigilance and care directly led to the Data Breach.

340. As a result of the Data Breach, Plaintiff Curry has and will continue to take reasonable precautions to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving a notice; monitoring her credit card and other financial statements for any signs of fraudulent activity; monitoring her credit report; managing the disruptive scam phone calls, texts, and emails on a daily basis. Plaintiff Curry has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Additionally, Plaintiff Curry has spent money in response to the Data Breach. Plaintiff Curry purchased Lifelock in response to the Data Breach.

341. Despite taking the precautionary measures and staying vigilant as recommended in the Data Breach notification letter, Plaintiff Curry has already experienced the effects of the dissemination of her PII on the Dark Web. As a result of the Data Breach, Plaintiff Curry has received multiple notices of suspicious activity from her credit monitoring service. Plaintiff Curry has also seen an increase in spam texts, emails, and phone calls since the breach.

342. To date, Plaintiff Curry has spent multiple hours on efforts to react to and protect herself from harm resulting from the Data Breach. Plaintiff Curry values her privacy and is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

343. Had Plaintiff Curry been informed of Mr. Cooper's insufficient data security measures to protect her PII, she would not have willingly provided his PII to Mr. Cooper. Given the highly sensitive nature of the PII stolen, and its subsequent dissemination to unauthorized parties, Plaintiff Curry has already suffered injury and remains at a substantial and imminent risk of future harm. As a result of the Data Breach, Plaintiff Curry anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach.

344. Plaintiff Curry suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

345. The Data Breach has caused Plaintiff Curry to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key

details about the Data Breach's occurrence.

346. As a result of the Data Breach, Plaintiff Curry is and will continue to be at increased risk of identity theft and fraud for years to come.

347. Plaintiff Curry has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

348. Upon information and belief, Mr. Cooper continues to store and/or share Plaintiff Curry's PII on its internal systems. Thus, Plaintiff Curry has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

349. Defendant Nationstar Mortgage LLC d/b/a Mr. Cooper ("Nationstar") is a limited liability company incorporated in Delaware, with its headquarters and principal place of business located at 8950 Cypress Waters Boulevard, Coppell, Texas 75019-4620. Nationstar is the operating subsidiary of parent Defendant Mr. Cooper Group, Inc. Nationstar is registered to do business with the Texas Secretary of State. The registered agent for service of process is Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

350. Defendant Mr. Cooper Group, Inc. is incorporated in Delaware with its principal place of business located at 8950 Cypress Waters Boulevard, Coppell, Texas 75019-4620. Mr. Cooper Group, Inc. is the operating parent of subsidiary Nationstar. Mr. Copper Group, Inc. is registered to do business with the Texas Secretary of State. The registered agent for service of process is Corporation Service Company d/b/a CSC – Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, TX 78701-3218.

JURISDICTION AND VENUE

351. This Court has jurisdiction over Plaintiffs' claims pursuant to 28 U.S.C. § 1332(d) because this a class action with diversity between at least one class member (including Plaintiffs) and one defendant, the aggregate amount of damages exceeds $5,000,000.00, and unnamed class members are citizens across the United States. This action therefore falls within the original jurisdiction of the federal courts pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). This Court also has original subject matter jurisdiction over federal claims because the amount in controversy exceeds $75,000 and there is complete diversity of citizenship pursuant 28 U.S.C. § 1332, and supplemental jurisdiction over all state-law claims under 28 U.S.C. § 1367.

352. This Court has personal jurisdiction over Mr. Cooper, which has its principal place of business in Dallas County, Texas. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b)–(c) because Defendants reside here and the events giving rise to Plaintiff's causes of action occurred in this District.

FACTUAL ALLEGATIONS

Mr. Cooper's Business

353. Mr. Cooper Group, Inc., formerly Nationstar Mortgage Holdings, Inc., was founded in Denver, Colorado, in 1994 as Nova Credit Corporation. In 1997, the company moved to Dallas, Texas, where home-builder Centex Homes established Nova Credit Corporation as their in-house lender for new construction and changed the company name to Centex Credit Corporation. In 2001, Centex Credit Corporation was merged into Centex Home Equity Company, and it operated as the subprime mortgage originator and servicer for Centex until 2005.

354. In 2005, the decision was made to withdraw Centex Homes from non-home-building businesses, including the mortgage business. Fortress Investment Group acquired Centex Home Equity and renamed it Nationstar Mortgage in 2006.

355. In March 2012, Nationstar Mortgage Holdings, Inc. went public with an initial public offering on the New York Stock Exchange.

356. Nationstar Mortgages, LLC, is the consumer-facing mortgage lender and servicer that operates under the service mark "Mr. Cooper". In August 2017, Nationstar Mortgage, LLC, announced it was changing its name to Mr. Cooper. The company stated that the name change was meant to "personalize the mortgage experience". In 2020, Mr. Cooper originated over 146,000 mortgages with a total value of over $36 billion.

357. Today, Mr. Cooper continues its focus as a loan servicer that "provides servicing, origination and transaction-based services related to single family residences throughout the United States."[1] Mr. Cooper is one of the largest home loan servicers and originators in the country, currently serving millions of customers and servicing loans worth some $937 billion, making it the largest servicer in the nation.[2] Frequently, home buyers are introduced to Mr. Cooper after their mortgage is sold or assigned to the company for servicing.

358. In the course of providing its services, Mr. Cooper collects and retains customers' highly sensitive Personally Identifiable Information ("PII" or "Private Information") and

[1] Mr. Cooper Group, Oct. 2023 Form 10-Q, https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/6ea7ec4e-5b61-47c1-b6d8-ba74e4ccd120.pdf (last visited Nov. 20, 2023).

[2] Cyberattack Disrupts Mortgage Payments for Millions of Mr. Cooper Customers, *New York Times* (Nov. 7. 2023), https://www.nytimes.com/2023/11/07/business/cyberattack-mr-cooper-mortgages.html.

regularly stores and transfers such information as part of its regular business operations. According to Mr. Cooper, this highly sensitive customer PII includes "names, phone numbers, email addresses, mailing address, approximate location, technology habits (e.g. what browser you use, if you are using a tablet or mobile phone, and internet activity), and commercial information like the products/services you've purchased from us," as well as Social Security numbers, employment history, and bank account numbers.[3] Mr. Cooper claims to collect this information directly from customers, internet advertisers, mortgage lead generators, other mortgage servicers, government entities, and cookies or other online tools and technology.

359. Mr. Cooper collects customer PII for a variety of purposes including "making and servicing mortgage loans," "performing services," "providing financing and customer service," "providing online products and services," "marketing and advertising." In Mr. Cooper's own words, "You could say that we collect, process, store and disclose your information."[4]

360. In its 2022 Annual Report, Mr. Cooper acknowledged the role PII plays in its business operations: "As a part of conducting business, we receive, transmit and store a large volume of personally identifiable information and other user data."[5]

361. By obtaining, collecting, and storing the PII of Plaintiffs and Class members, Mr. Cooper assumed legal and equitable duties and knew or should have known it was responsible

---

[3] Mr. Cooper Group, California Consumer Privacy Act, https://www.mrcooper.com/privacy/ccpa (last visited Nov. 20, 2023).

[4] *Id*.

[5] Mr. Cooper Group 2022 Annual Report, https://s1.q4cdn.com/275823140/files/doc_financials/2022/ar/book-marked-annual-report-final.pdf (last visited Nov. 20, 2023).

for protecting the PII from unauthorized disclosure. Plaintiffs and Class members relied on Mr. Cooper to keep their information confidential and secure.

362. Mr. Cooper maintains a privacy policy accessible from its website ("Privacy Policy"). The Privacy Policy states that "customer service, trust and confidence is a high priority. That's why we welcome this opportunity to describe our privacy policies, the steps we take to protect and maintain your information and to let you know how you can choose how your customer information may be shared."[6] It further states that "[k]eeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit disclosure by maintaining physical, electronic and procedural safeguards."[7]

363. In the same policy, Mr. Cooper represents that the same protections will apply to former Mr. Cooper customers. Unfortunately, Mr. Cooper did not abide by its promises to keep customers' PII secure. Instead – as evidenced by its loss of control of its customers' data – Mr. Cooper never implemented the security safeguards sufficient to fulfill those duties, failing to adequately train its employees on data security, develop policies to prevent breaches, enforce those policies, follow industry standard guidelines on cybersecurity, and timely respond to data breaches and inform customers as required by law. As a result, Mr. Cooper left customers' PII a vulnerable target for theft and misuse.

---

[6]Mr. Cooper Group, Privacy Policy, https://www.mrcooper.com/privacy (last visited Nov. 20, 2023).

[7] Mr. Cooper Group, Privacy Policy, https://www.mrcooper.com/privacy (last visited Nov. 20, 2023).

Defendants' Disclosure of the Data Breach

364. This claim arises from a data breach discovered by Defendants on or about October 31, 2023 (the "Data Breach").

365. On November 1, 2023, Mr. Cooper sent a communication to customers stating that "We are currently experiencing a technical outage that may delay your payment this month. Rest assured, you will not be charged any late fees or incur any penalties due to this issue. Once your payment is processed, you will receive a confirmation."

366. On November 2, 2023, Mr. Cooper sent another communication stating that: "On October 31st, Mr. Cooper became the target of a cyber security incident and took immediate steps to lock down our systems in order to keep your data safe. We are working to resolve the issue as quickly as possible." It provided a link to its website which provided the following additional information:[8]

> As part of our ongoing investigation, we now believe that ***certain customer data was exposed***. We are continuing to investigate precisely what information was exposed. In the coming weeks, we will mail notices to any affected customer and provide them with complimentary credit monitoring services.

367. This communication from Mr. Cooper has been repeatedly updated in contradictory and incomplete ways. As of November 10, 2023, Mr. Cooper claimed the impacted systems did not store customer financial information: "Please note that Mr. Cooper does not store banking information related to mortgage payments on our systems. This information is hosted

[8] Ionut Arghire, "Mr. Cooper Says Customer Data Compromised in Cyberattack" (November 13, 2023), https://www.securityweek.com/mr-cooper-says-customer-data-compromised-in-cyberattack/ (last accessed on June 26, 2024), emphasis added.

with a third-party provider and, based on the information we have to date, we do not believe it was affected by this incident." On November 15, 2023, Mr. Cooper removed that language from its online notice.[9]

368. Mr. Cooper's securities filings similarly leave many unanswered questions. On November 2, 2023, Mr. Cooper filed a Form 8-K with the U.S. Securities and Exchange Commission ("SEC") disclosing the cyberattack in which an unauthorized third party gained access to its systems. Through its investigation, Mr. Cooper determined that "there was unauthorized access to certain of [their] systems between October 30, 2023 and November 1, 2023." Mr. Cooper stated that it "initiated response protocols, including deploying containment measures to protect systems and data and shutting down certain systems as a precautionary measure."[10]

369. Mr. Cooper stated in its filing that it did not believe that the incident would have a material adverse effect on its business, operations or financial results.[11] Additionally, in the aftermath of the Data Breach, Mr. Cooper failed to indicate any measures they had taken to

---

[9] *Mortgage Giant Mr. Cooper Says Customer Data Exposed in Breach*, https://www.bleepingcomputer.com/news/security/mortgage-giant-mr-cooper-says-customer-data-exposed-in-breach/ (last visited Nov. 20, 2023).

[10] *Id.*

[11] Id. Mr. Cooper Group Inc., Form 8-K, (Nov. 2, 2023) https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/51b7c580-cebd-4fa6-8d5b-f22bb7da7c5f.pdf (last visited June 13, 2024).

mitigate the harm beyond "locking down [their] systems, changing account passwords, and restoring systems."[12]

370. On November 8, 2023, Mr. Cooper filed a supplemental report with the SEC, this time admitting that its analysis revealed that "***customer data was exposed***."[13] Mr. Cooper continued to maintain that its financial condition would not be materially impacted by the Data Breach

371. About a month later, on December 15, 2023, Mr. Cooper told regulators the truth: "Our forensic review determined that personal information relating to substantially all current and former customers ***was obtained*** from our systems during this incident."[14] Mr. Cooper also confirmed in a regulatory notice filed with the Maine Attorney General's office that 14,690,284 customers' data was compromised, including names, addresses, phone numbers, Social Security numbers, dates of birth and bank account numbers.

372. On the same day—December 15, 2023—Mr. Cooper issued a Notice of Cybersecurity Incident on its website and emailed the Data Breach Notice, discussed in more detail below, to its customers. In the Data Breach Notice, Defendants stated that they believed that customer data *was exposed* and advised customers to monitor their financial accounts and

---

[12] *See* Maine Attorney General, "Data Breach Notifications: Nationstar Mortgage LLC (dba Mr. Cooper)," https://apps.web.maine.gov/online/aeviewer/ME/40/176a338a-f640-43d5-b975-5996823e7ce4.shtml (last accessed June 26, 2024).

[13] Mr. Cooper Group Inc., Form 8-K/A (Nov. 8, 2023) https://d18rn0p25nwr6d.cloudfront.net/CIK-0000933136/4edccf79-a641-4e5a-bf8c-0d681457778c.pdf last visited June 13, 2024).

[14] December 15, 2023, email from Chief Risk & Compliance Officer Meredith Coffman to State Assistant Attorneys General.

credit reports for unauthorized activity.[15]

373. In the Data Breach Notices mailed to various customers, Defendants confirmed that the affected information included: customer names, addresses, phone numbers, Social Security numbers, dates of birth, and bank account numbers. The fact that criminals were able to access and steal this data suggests that Defendants stored customer PII in a manner that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration.

1. Mr. Cooper's Failures to Secure Its Clients' Data Allowed the Data Breach to Occur

374. A series of cybersecurity failures and refusal to follow basic cyber hygiene norms permitted the cybercriminal to access Mr. Cooper's systems and victimize Class Members.

375. Contrary to industry-standard practices, Mr. Cooper improperly failed to encrypt Plaintiffs' and Class Members' PII, or used deprecated encryption protocols, failed to delete such PII after it no longer needed to be retained, stored it in a vulnerable, internet-accessible environment, failed to deploy and calibrate up-to-date authentication measures for user credentials, failed to apply the requisite "patches" to its critical software to eliminate known vulnerabilities, and failed to monitor traffic on its network in an effort to detect malicious activity.

376. In this case, Defendants were subject to two-stage attack: first, by an initial access broker ("IABs") which penetrated their system through multiple access points and exfiltrated customer PII, and then by a ransomware gang which sought and extracted a ransom.

---

[15] Maine Attorney General, "Data Breach Notifications: Nationstar Mortgage LLC (dba Mr. Cooper)", https://apps.web.maine.gov/online/aeviewer/ME/40/176a338a-f640-43d5-b975-5996823e7ce4.shtml (last accessed June 26, 2024).

Phase 1: IAB Attack

377. A leading cybersecurity blog explains that "IABs offload the difficult work of finding targets and gaining access. In doing so, they enable ransomware groups to attack at scale because they're not wasting time trying to secure a foothold in target networks […] They can immediately procure that access via an IAB and get to work encrypting [the victim's] data."[16]

378. Once IABs establish a foothold in the target's systems, and validate the ability to compromise and exfiltrate data, they develop custom software, or RaaS ("Ransomware as a service), which they sell to cybercriminals engaged in ransomware attacks.

379. As reported in industry press, "some IABs work directly for ransomware groups or affiliates of RaaS groups. This significantly speeds up a ransomware attack, as affiliates can leverage procured access and jump almost immediately to conducting their attack rather than wasting time gaining access." The IAB then passes access to the RaaS affiliate, who then launches the ransomware attack.[17] As a result, by the time the ransomware attack is launched, the data is often already exfiltrated from the system.

380. On information and belief, IAB cybercriminals were able to access Mr. Cooper's network through multiple channels – using compromised credentials, a compromised public-facing website, and a compromised IP telephone system.

381. Specifically, Plaintiffs' investigation reveals that IABs accessed Mr. Cooper's

---

[16] Center for Internet Security, "initial Access Brokers How They're Changing Cybercrime", https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime (last accessed on June 26, 2024).

[17] *Id*.

network using a compromised credential through a ".dev" site (a development site, or a version of the public-facing website that has been replicated for development and testing) located in India. In a separate access point, IABs accessed the Mr. Coper's network through an out-of-date Avaya IP phone system that connected into Mr. Cooper's call center. Compromised IBM Identity Guard credentials and Citrix credentials were yet another point through which IABs gained access to Mr. Cooper's network.

382. Notably, in an egregious breach of cybersecurity protocols, Mr. Cooper's systems were missing multi-factor authentication ("MFA") all through calendar year 2022. MFA has been an industry standard in the financial sector since 2018. Authentication controls such as MFA help to ensure access to confidential information are only granted to those authorized. Failure to institute industry standard authentication protocols enabled cybercriminals to penetrate Defendants' system through multiple channels.

383. Zone-H, an Estonian archive of defaced websites, revealed that the web domain mrcooper.com had suffered a defacement attack as a direct result of misconfiguration of the consumer-facing web site as early as May 2023.

384. A defacement attack of a website is a cyberattack in which malicious actors replace portions or all content on a website with their own messages, links, and content. Common causes of defacement attacks are unauthorized access, lack of secure access to underlying code and databases (such as SQL injections), vulnerable applications subject to

malware and domain hijacking from poorly configured domains.[18]

385. During the relevant time described herein, the mrcooper.com website redirected to an older Nation Star Mortgage domain - thenationstarmtg.com. User accounts for this older domain were advertised for sale on hacker forums, on or before March 1, 2023. The fact that the domain was announced as "captured" and for sale in March 2023, means that the initial attack likely occurred between 6 months to 2 years prior to that date.

386. Having "captured" Mr. Cooper's public-facing website, Mr. Cooper's consumers' login credentials were found on the "dark web" and posted by threat actors on various hacker forums. This suggests that the credentials, or passwords, used by mortgagees were either not protected at all, or used "deprecated" encryption or hashing protocols which are vulnerable to brute-force attacks using modern computing power.

387. Discussions on hacker forums suggest that CobaltStrike malicious software was used to perpetrate this cyberattack. This software was well known by 2023, but Mr. Cooper failed to identify its penetration into its systems.

Phase 2: Ransomware Attack

388. Having established a foothold in Mr. Cooper's network, cybercriminals moved on to the next stage of their attack, in which they developed and deployed RaaS software on behalf of a ransomware group.

389. Upon information and belief, the Ransomware group seized control of Mr.

[18] Imperva. "Website Defacement Attack: What is Website Defacement", https://www.imperva.com/learn/application-security/website-defacement-attack/ (last accessed on June 26, 2024).

Cooper's network and demanded payment for (1) releasing control of Mr. Cooper's network and (2) deleting Mr. Cooper's customer data in its possession. Such payment was provided. However, Mr. Cooper's customers' data remains in the possession of cybercriminals.

390. Ransomware is a known threat that preys on unpatched and unprotected systems. One of the first lines of defense against ransomware is to ensure the latest patches are applied immediately. Defendants failed to update their systems with the requisite "patches" in a timely way, or at all. The common vulnerabilities and exposures ("CVEs") associated with Mr. Cooper / Nation Star cyberattack include CVE-2014-3566, 2016-0204 (IBM cloud orchestrator), 2016-0800 (invalid or deprecated certs), 2016-2000 (asset management system for software that runs on HP servers).

391. Upon information and belief, Defendants were subject to a successful ransomware attack and paid ransom to cybercriminals before it could restore access to their own systems.

392. The fact that Defendants paid ransom to the cybercriminals indicates that (1) Defendants' security was unable to detect or prevent an attack that was able to traverse its systems with minimal notice; and (2) Defendants did not have a qualified incident response plan to deal with a ransomware attack, a very common type of cyberattack.

393. Typically, even if the ransom were paid, customer data is still sold and used. Ransomware attacks typically do not begin with the ransomware group finding the vulnerability. Rather, the attack typically begins with initial access brokers ("IABs") that work for multiple groups, including nation states, finding, validating and exfiltrating the data from the organization. Thus, even if the ransomware group does not exfiltrate the data, the data is nearly always taken *before* the ransomware group penetrates and extorts.

394. Data from a large number of organizations which recently paid ransom to cybercriminals was nevertheless leaked online, including:[19]

a. FatFace (2021): The UK-based clothing retailer was attacked in January 2021 and paid a $2 million ransom. However, despite the payment, customer data was reportedly leaked online.

b. CNA Financial (2021): CNA Financial, one of the largest insurance companies in the US, paid a $40 million ransom after a ransomware attack in March 2021. Despite the payment, some data was leaked online.

c. Quanta Computer (2021): This Taiwanese manufacturer, a supplier for Apple, was hit by the REvil ransomware group in April 2021. Despite paying the ransom, some of the schematics and internal documents related to Apple products were leaked online.

d. Kingfisher Insurance (2023): In early 2023, the hackers leaked sensitive customer information from this Australian insurance company despite the company paying a ransom.

e. Australian Clinical Labs (2023): Another Australian entity, Australian Clinical Labs, experienced a ransomware attack in 2023. Despite the payment, patient data was leaked.

f. MoveIt (2023): The MoveIt data transfer software, used by numerous

[19] See, generally, PhishLabs. Digital Risk Protection., "Ransomware Groups Break Promises, Leak Data Anyway" (November 25, 2020), https://www.phishlabs.com/blog/ransomware-groups-break-promises-leak-data-anyway

organizations, was breached in late 2023. Several companies using MoveIt paid ransoms, but the attackers still leaked sensitive data, affecting thousands of users across different organizations.

g. Enzo Biochem (2023): Enzo Biochem, a diagnostics company, experienced a ransomware attack in late 2023. Despite paying a ransom, the attackers leaked patient data and sensitive company information.

h. Steris (2024): In early 2024, Steris, a medical equipment company, faced a ransomware attack. After paying the ransom, the company discovered that the attackers had already leaked proprietary information and sensitive data.

395. As Defendants admitted, Class Members' PII was stolen in the cyberattack. Given the above precedents, it is likely that, by the time Defendants made a payment to cybercriminals holding their clients' PII for ransom, the data had already been exfiltrated.

Following the Breach, Defendants' Clients'
Login Credentials and Hacking Software Remain for Sale

396. Starting on or about June 9, 2024, the cybercriminal Wockstar, likely the IAB and RaaS code developer behind the Data Breach, began selling the source code allegedly used to perpetrate the Data Breach for $50,000 in bitcoin.

397. Wockstar's post describes the technological components used to perpetrate the attack in detail, including a "lock & unlock programmed in Rust", "XChaCha8Poly1305 Encryption (2.5x faster than regular ChaCha20)," "Affiliate Panel & Admin Panel written in PHP" and other modules.

398. The posted information identifies methods of access, egress and ingress ports,

usernames and passwords used by the attacker in the Data Breach.

399. The cybercriminal Wockstar even offered for sale an instructional video showing how the Data Breach was perpetrated.

400. The technical details provided by the cybercriminal Wockstar prove that, despite paying ransom, Defendants' clients' PII was exfiltrated from Defendants by cybercriminals. Either Defendants had no firewall to protect against such an intrusion and exfiltration, or its firewall was bypassed and disabled during the cyberattack.

Even Following the Breach, Defendant Left Client
Data Exposed in a Google Cloud Storage Bucket

401. Even after the Data Breach was exposed, Defendants continued to handle their customers' PII in a careless manner. On February 22, 2024, it was reported that Defendants left PII belonging to some two million of its customers on an open Google Cloud storage bucket, where it was "accessible to anyone willing to look." The data included names, customer IDs, loan numbers, email addresses and phone numbers.[20]

402. In an internal memorandum on February 23, 2024, Mr. Cooper admitted that it was this cybersecurity news outlet that had to inform Mr. Cooper about its own carelessness, stating that "[r]esearchers at Cybernews contacted Mr. Cooper on February 8, 2024, making us aware that they had discovered publicly accessible files on Google Cloud housing some customer information."

[20] Vilius Petkauskas, "Mr. Cooper leak exposes over two million customers" (February 22, 2024), https://cybernews.com/security/mrcooper-leak-exposes-millions-customers/ (last accessed June 26, 2024).

403. Emphasizing its own inadequate data security measures, Mr. Cooper admitted in its memorandum that it had been "working tirelessly to further secure our perimeter defenses and protect our network."

404. This further demonstrates the lack of basic cybersecurity measures and a culture of disregard for clients' PII, which remains pervasive at Defendants' business.

Data Breach Was Foreseeable and Preventable

405. Mr. Cooper's failure to prevent the breach is inexcusable given its knowledge, prior to the breach, that financial services companies were a prime target for cyberattacks due to the vast amounts of PII they hold.

406. In March 2022, Bloomberg described the financial services industry as experiencing an "unrelenting year of fighting off cyber threats," and warned financial services providers "should expect more of the same or even worse."[21] As noted in the article, the Financial Services Information Sharing and Analysis Center's ("FS-ISAC") annual report on cyber threats predicted "current trends to continue and possible worsen over the next year," stating cybersecurity is "no longer just a back-office cost." These increases are "due to several factors," including the "rapid digitization of financial services, which accelerated during the pandemic," and "increased entry points for cyber criminals to possibly exploit." Teresa Walsh, who leads FS-ISAC's global intelligence office, described the financial sector as experiencing "a dizzying number of vulnerabilities."

[21] *Financial Firms Brace for More Cyber Threats After Trying 2021*, BLOOMBERG (March 10, 2022), https://www.bloomberg.com/news/articles/2022-03-10/financial-firms-poised-for-worse-cyber-threats-after-trying-year (last visited Nov. 20, 2023)

407. Mr. Cooper recognized this risk in its own regulatory filings. For example, in its 2022 Annual Report, Mr. Cooper acknowledged the business risk of suffering a cybersecurity incident:

> ***Cybersecurity risks for the financial services industry have increased significantly in recent years*** due to new technologies, the reliance on technology to conduct financial transactions and the increased sophistication of organized crime and hackers. Those parties also may attempt to misrepresent personal or financial information to obtain loans or other financial products from us or attempt to fraudulently induce employees, customers, or other users of our systems to disclose confidential information in order to gain access to our data or that of our customers.
>
> ***
>
> ***We and others in our industry are regularly the subject of attempts by attackers to gain unauthorized access to our networks, systems, and data, or to obtain, change, or destroy confidential data (including personal identifying information of individuals)*** through a variety of means, including computer viruses, malware, phishing, ransomware and other attack vectors. These attacks may result in unauthorized individuals obtaining access to our confidential information or that of our customers, or otherwise accessing, damaging, or disrupting our systems or infrastructure.
>
> ***
>
> ***A successful penetration or circumvention of the security of our or our vendors' systems or a defect in the integrity of our or our vendors' systems or cybersecurity could cause serious negative consequences for our*** business, including significant disruption of our operations, ***misappropriation of our confidential information or that of our custome***rs, or damage to our computers or operating systems and to those of our customers and counterparties"[22]

408. Mr. Cooper also witnessed numerous high-profile cybersecurity incidents affecting other companies in the financial services sector, including: credit reporting agency

[22]Mr. Cooper Group 2022 Annual Report, https://s1.q4cdn.com/275823140/files/doc_financials/2022/ar/book-marked-annual-report-final.pdf (last visited Nov. 20, 2023), emphasis added.

Equifax (147 million customers impacted, September 2017), Heartland Bank (130 million customers, January 2008), Capital One Bank (100 million customers, March 2019),[23] JPMorgan Chase (83 million customers, October 2014), Experian (24 million customers, August 2020), First American Financial (885 million customers, May 2019), and Flagstar Bank (1.5 million customers, June 2022), among scores of others.

409. Consequently, Mr. Cooper should have known of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs that would be imposed on customers as a result of a breach.

410. But despite all of the publicly available knowledge of the continued risks to client PII, and despite holding PII of millions of customers, Mr. Cooper failed to use reasonable care in maintaining the privacy and security of PII of Plaintiffs and Class Members.

411. Had Mr. Cooper implemented industry standard security measures and adequately invested in data security, unauthorized parties likely would not have been able to access Mr. Cooper's systems and the Data Breach would have been prevented or much smaller in scope.

Defendants Failed to Comply with FTC Guidelines

412. The Federal Trade Commission ("FTC") has promulgated numerous guides for

[23] Capital One was assessed an $80 million civil penalty by the Office of the Comptroller of the Currency ("OCC") due to its "failure to establish effective risk assessment processes prior to migrating significant information technology operations to the public cloud environment and the bank's failure to correct the deficiencies in a timely manner." OCC Assesses $80 Million Civil Money Penalty Against Capital One, OFFICE OF THE COMPTROLLER OF THE CURRENCY (Aug. 6, 2020), available at https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html (last visited Nov. 20, 2023)

businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

413. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[24] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[25]

414. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

415. The FTC has brought enforcement actions against financial entities for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

---

[24] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[25] *Id.*

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

416. Defendants failed to properly implement basic data security practices.

417. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

418. Defendants were at all times fully aware of their obligation to protect the Private Information of consumers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Regulations and Industry Standards

419. As shown above, experts studying cybersecurity routinely identify financial services providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

420. Defendants' inadequate data security measures violated applicable rules, regulations, and standards regarding data security. By not taking adequate security measures, Defendants violated the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, *et seq*., and the industry best practices that the GLBA requires for financial institutions.

421. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A). Mr. Cooper qualifies as a financial institution

under this definition and hence is subject to the GLBA.

422. Defendants collect nonpublic PII, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant period Defendants were subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated under the GLBA.

423. Defendants were at all times fully aware of their obligation to protect the Private Information of consumers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

424. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version taking effect on October 28, 2014.

425. Accordingly, Defendants' conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

426. Further, the Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and

integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendants were subject to the Safeguard Rule, and violated the Safeguard Rule.

427. Defendants failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

428. Defendants' conduct resulted in myriad failures to follow GLBA-mandated rules and regulations, many of which are also industry standard.

429. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

430. Other best cybersecurity practices that are standard in the financial industry include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems;

protection against any possible communication system; and training staff regarding critical points.

431. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

432. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

433. Cyberattacks and data breaches at financial service providers like Mr. Cooper are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

434. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[26]

[26] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

435. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

436. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

437. Identity thieves use stolen Private Information such as Social Security numbers

[27] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited June 13, 2024).

for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud, among others.

438. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

439. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[28]

440. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

441. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

442. According to the U.S. Government Accountability Office, which conducted a

[28] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, ***once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29, emphasis added.

443. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

444. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for the remainder of their lives.

445. PII can sell for as much as $363 per record according to the Infosec Institute.[29] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

446. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud

---

[29] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[30] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.

may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

447. Moreover, it is almost impossible to change or cancel a stolen Social Security number.

448. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

449. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are

[31] *Id.*

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

worth more than 10x on the black market."[33]

450. Because of the value of their collected and stored data, businesses entrusted with valuable Private Information have experienced disproportionally higher numbers of data theft events than other industries.

451. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

CLASS ACTION ALLEGATIONS

452. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Class") and state subclasses ("Subclasses"):

Nationwide Class

All individuals residing in the United States whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

California Subclass

All individuals residing in California whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Florida Subclass

[33] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

All individuals residing in Florida whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

North Carolina Subclass

All individuals residing in North Carolina whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

New York Subclass

All individuals residing in New York whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Nevada Subclass

All individuals residing in Nevada whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Illinois Subclass

All individuals residing in Illinois whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Montana Subclass

All individuals residing in Montana whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Missouri Subclass

All individuals residing in Missouri whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Alabama Subclass

All individuals residing in Alabama whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Texas Subclass

All individuals residing in Texas whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Georgia Subclass

All individuals residing in Georgia whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Minnesota Subclass

All individuals residing in Minnesota whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Louisiana Subclass

All individuals residing in Louisiana whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Washington Subclass

All individuals residing in Washington whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

Colorado Subclass

All individuals residing in Colorado whose PII was accessed and/or acquired as a result of the Data Breach announced by Mr. Cooper in or around November 2023.

453. Specifically excluded from the Class are Mr. Cooper and its officers, directors, or employees; any entity in which Mr. Cooper has a controlling interest; and any affiliate, legal representative, heir, or assign of Mr. Cooper. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

454. **Jurisdictional Amount**. As alleged herein, Plaintiffs seek damages on behalf of themselves and potentially millions of putative class members, satisfying the $5 million jurisdictional requirement of 28 U.S.C. § 1332(d)(2).

455. **Ascertainability**. The members of the Class are readily identifiable and ascertainable. Mr. Cooper and/or its affiliates, among others, possess the information to identify and contact Class members.

456. **Numerosity**. Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all of them is impracticable. Mr. Cooper's statements reveal that the Class potentially contains millions of individuals whose PII was compromised in the Data Breach.

457. **Typicality**. Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of all Class members because they were customers of Mr. Cooper, impacted by the Data Breach, and suffered harm as a result.

458. **Adequacy of Representation**. Federal Rule of Civil Procedure 23(a)(4). Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class members' interests. Plaintiffs were subject to the same Data Breach as Class members, suffered similar harms, and face similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including scores of data breach and privacy cases.

459. **Commonality and Predominance**. Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). There are questions of law and fact common to the Class such that there is a well-

defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

a. Whether Mr. Cooper owes Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII

b. Whether Mr. Cooper acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;

c. Whether Mr. Cooper violated its duty to implement reasonable security systems to protect Plaintiffs' and Class members' PII;

d. Whether Mr. Cooper's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members;

e. Whether Mr. Cooper provided timely notice of the Data Breach to Plaintiffs and Class members; and

f. Whether Plaintiffs and Class members are entitled to compensatory damages, punitive damages, and/or nominal damages as a result of the Data Breach.

460. Mr. Cooper has engaged in a common course of conduct and Plaintiffs and Class members have been similarly impacted by Mr. Cooper's failure to maintain reasonable security procedures and practices to protect customers' PII.

461. **Superiority**. Federal Rule of Civil Procedure 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class

treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF ON BEHALF OF THE CLASS

COUNT I
Breach of Express Contract

462. Plaintiffs repeat and reallege every allegation set forth in paragraphs 1 through 461.

463. Mr. Cooper's Privacy Policy is an agreement between Mr. Cooper and individuals who provided their PII to Mr. Cooper, including Plaintiffs and Class members.

464. Mr. Cooper represents that its Privacy Policy applies to information it collects about individuals who seek, apply for, or obtain Mr. Cooper's financial products and services.

465. Mr. Cooper's Privacy Notice stated at the time of the Data Breach that Mr. Cooper "use[s] security measures that comply with federal law," and "[t]hese measures include computer safeguards and secured files and buildings," in order to "protect your personal information from unauthorized access and use."

466. Mr. Cooper further agreed at the time of the Data Breach that it would only share

data under certain enumerated circumstances, which include: "[f]or our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus," "[f]or our marketing purposes – to offer our products and services to you," "[f]or joint marketing with other financial companies," and "[f]or our affiliates' everyday business purposes – information about your transactions and experiences."

467. None of the enumerated circumstances involve sharing Plaintiffs or the Class Members' PII with unauthorized parties.

468. Plaintiffs and Class Members on the one side and Mr. Cooper on the other formed a contract when Plaintiffs and Class Members obtained services from Mr. Cooper, or otherwise transmitted or authorized the transmission of PII to Mr. Cooper subject to its Privacy Policy.

469. Plaintiffs and Class Members fully performed their obligations under the contracts with Mr. Cooper.

470. Mr. Cooper breached its agreement with Plaintiffs and Class Members by failing to protect their PII. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of the agreement.

471. As a direct and proximate result of Mr. Cooper's breach of contract, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT II
Breach of Implied Contract

472. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461 and assert this claim in the alternative to their breach of contract claim to the extent necessary.

473. Mr. Cooper acquired and maintained the PII of Plaintiffs and the Class that it received either directly from Plaintiffs and the Class or indirectly from other mortgage originators.

474. When Plaintiffs and Class Members paid money and provided their PII to their mortgage originators, either directly or indirectly, in exchange for services, they entered into implied contracts with their mortgage originators and their business associates, including Mr. Cooper.

475. As part of these transactions, Mr. Cooper agreed to safeguard and protect the PII of Plaintiffs and Class Members. Implicit in the transactions between Mr. Cooper and Class members was the obligation that Mr. Cooper would utilize reasonable measures to keep the PII secure; Mr. Cooper would limit access to PII; Mr. Cooper would use the PII for approved business purposes only; and Mr. Cooper would retain PII only as necessary to perform necessary business functions.

476. Additionally, Mr. Cooper implicitly promised to retain this Plaintiffs' and Class Members' PII only under conditions that kept such information secure and confidential.

477. Further, the implied contracts included Defendants' representation in their Privacy Policy that: "Keeping financial information is one of our most important responsibilities. Only those persons who need it to perform their job responsibilities are authorized to access your information. We take commercially reasonable precautions to protect your information and limit

disclosure by maintaining physical, electronic and procedural safeguards. . . . This policy is provided by Mr. Cooper and its subsidiaries."

478. Plaintiffs and Class Members believed that Mr. Cooper would use part of the monies paid directly or indirectly to Mr. Cooper under the implied contracts to fund adequate and reasonable data security practices to protect their PII.

479. Plaintiffs and Class Members would not have provided and entrusted their PII to Mr. Cooper or would have paid less for Mr. Cooper's services in the absence of the implied contract between them and Mr. Cooper. The safeguarding of Plaintiffs' and Class Members' PII was critical to realizing the intent of the parties.

480. Mr. Cooper breached its implied contract with Plaintiffs and Class Members by failing to reasonably safeguard and protect their PII, which was compromised as a result of the Data Breach.

481. As a direct and proximate result of Mr. Cooper's breach of implied contract, Plaintiffs and Class Members sustained actual losses and damages as alleged herein, including that they did not receive the benefits of the bargains for which they paid. Plaintiffs and class members alternatively seek an award of nominal damages.

COUNT III
Negligence

482. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461.

483. Upon accepting transmission of Plaintiffs' and Class Members' PII, Mr. Cooper owed a common law duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties.

Mr. Cooper owed a duty to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, to design, implement, and monitor data security systems, policies, and processes to protect against foreseeable threats, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected customers' PII.

484. Mr. Cooper owed this duty to Plaintiffs and Class Members because Mr. Cooper collected their PII in the course of its business and it was reasonably foreseeable that Plaintiffs and Class Members would be harmed if Mr. Cooper failed to keep their PII secure.

485. Pursuant to this duty, Mr. Cooper was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiffs and the Class. Mr. Cooper further owed to Plaintiffs and the Class a duty to implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

486. Mr. Cooper was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

487. Mr. Cooper's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers.

488. Mr. Cooper's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and common law described above, but also because Mr. Cooper is bound by industry standards to protect confidential PII.

489. The imposition of a duty of care on Mr. Cooper to safeguard the PII they maintained is appropriate because any social utility of Mr. Cooper's conduct is outweighed by

the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

490. Mr. Cooper breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII. Mr. Cooper's negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email systems had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Plaintiffs' and Class Members' Private Information;

f. Failing to detect in a timely manner that Plaintiffs' and Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

491. It was foreseeable that Mr. Cooper's failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

492. Plaintiffs and Class members are a well-defined, foreseeable, and probable group of consumers that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

493. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII would result in one or more types of injuries to Plaintiffs and Class members.

494. But for Mr. Cooper's wrongful and negligent breach of duties owed to Plaintiffs and Class members, Plaintiffs' and Class Members' PII would not have been compromised

495. As a direct and proximate result of Mr. Cooper's negligence, Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach, including, but not limited to: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services necessitated by Mr. Cooper's data breach; and (ix) any nominal damages that may be awarded.

COUNT IV
Negligence *Per Se*

496. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461.

497. Pursuant to Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, Mr. Cooper had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

498. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Mr. Cooper, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

499. Mr. Cooper violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. Mr. Cooper's conduct was unreasonable given the nature and amount of PII it obtained, stored, and disseminated in the regular course of its business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members if their PII was exposed.

500. The harms that occurred as a result of the Data Breach are the types of harms the FTC Act was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiffs and Class members here.

501. Mr. Cooper likewise violated the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 et

seq.) ("GLBA"), its Privacy Rule and/or Regulation P, and its Safeguards Rule by, among other things: (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's internal systems that were inadequately secured; (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on such an insecure platform and/or system; (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information; (d) failing to adequately (i) test and/or monitor the system were the Data Breach occurred and (ii) update and/or further secure its data security practices in light of the heightened risk environment; and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of millions individuals with one or more non-affiliated third parties.

502. Mr. Cooper's violations of Section 5 of the FTC Act and the GLBA constitute negligence *per se*.

503. Plaintiffs and Class Members are within the class of persons these federal laws were designed to protect.

504. Mr. Cooper knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, Mr. Cooper's vulnerability to network attacks, and the importance of adequate security.

505. Mr. Cooper breached its duty to Plaintiffs and Class Members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class

Members;

b. Failing to comply with industry standard data security measures leading up to the Data Breach;

c. Failing to comply with its own Privacy Policy;

d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Mr. Cooper's network and systems;

f. Failing to recognize in a timely manner that PII had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

506. Plaintiffs' and Class Members' PII would not have been compromised but for Mr. Cooper's wrongful and negligent breach of its duties.

507. Mr. Cooper's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that financial service providers are prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by Mr. Cooper.

508. It was also foreseeable that Mr. Cooper's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class Members.

509. As a direct and proximate result of Mr. Cooper's negligence *per se*, Plaintiffs and

Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach, including but not limited to: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (viii) the present value of ongoing credit monitoring and identity defense services necessitated by Mr. Cooper's data breach; and (ix) any nominal damages that may be awarded.

COUNT V
Unjust Enrichment

510. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461 and assert this claim in the alternative to their breach of contract claims to the extent necessary.

511. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, used by, and maintained by Mr. Cooper and that was ultimately stolen in the Mr. Cooper data breach.

512. Plaintiff and Class Members provided their PII to Mr. Cooper and paid Mr. Cooper a certain sum of money, which was used to fund data security.

513. On information and belief, Mr. Cooper funds its data security measures entirely from its general revenue, including from revenues it generates based on protecting Plaintiff's and Class Members' PII.

514. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members to Mr. Cooper was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Mr. Cooper.

515. Mr. Cooper benefited from the conferral upon it of the PII pertaining to Plaintiffs and the Class Members and by its ability to retain, use, and profit from that information. Mr. Cooper understood and valued this benefit.

516. Mr. Cooper also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Mr. Cooper maintaining the privacy and confidentiality of that PII.

517. Without Mr. Cooper's willingness and commitment to maintain the privacy and confidentiality of the PII, that PII would not have been transferred to and entrusted to Mr. Cooper. Further, if Mr. Cooper had disclosed that their data security measures were inadequate, it would not have been permitted to continue in operation by regulators or its customers.

518. Mr. Cooper admits that it uses the PII it collects for, among other things: "marketing and promotional communications."

519. Mr. Cooper was unjustly enriched by profiting from the use of Plaintiffs' and Class Members' PII as well as the services and products it was able to market, sell, and create under the false pretense it had adequate systems in place to protect customers' PII to the

detriment of Plaintiffs and the Class.

520. Mr. Cooper also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII and profits it gained through the use of Plaintiffs' and Class members' PII.

521. As a result of Mr. Cooper wrongful conduct, Mr. Cooper has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members.

522. It is inequitable, unfair, and unjust for Mr. Cooper to retain these wrongfully obtained benefits. Mr. Cooper's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

523. Plaintiffs and Class Members have no adequate remedy at law.

524. Mr. Cooper is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Mr. Cooper as a result of its wrongful conduct, including specifically: the value to Mr. Cooper of the PII that was stolen in the Data Breach; the profits Mr. Cooper received and is receiving form the use of that information; the amounts that Mr. Cooper overcharged Plaintiffs and Class Members for use of Mr. Cooper's products and services; and the amounts that Mr. Cooper should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT VI
Invasion of Privacy

525. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461.

526. Plaintiffs and Class Members shared PII with Mr. Cooper and/or its affiliates that Plaintiffs and Class Members wanted to remain private and non-public.

527. Plaintiffs and Class Members reasonably expected that the PII they shared with Mr. Cooper would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

528. Mr. Cooper intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a criminal third party.

529. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Mr. Cooper unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosures of their PII without consent.

530. Plaintiffs' and Class Members' PII that was compromised during the Data Breach was highly sensitive, private, and confidential, as it likely included Social Security numbers and other information that is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it.

531. Mr. Cooper's intrusions into Plaintiffs' and Class Members' seclusion were

substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

532. As a direct and proximate result of Mr. Cooper's invasion of privacy, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT VII
Breach of Confidence

533. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461.

534. Plaintiffs and Class members maintained a confidential relationship with Mr. Cooper whereby Mr. Cooper undertook a duty not to disclose PII provided by Plaintiffs and Class Members to unauthorized third parties. Such PII was confidential, novel, highly personal and sensitive, and not generally known.

535. Mr. Cooper knew Plaintiffs' and Class Members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

536. Plaintiffs' and Class Members' PII was disclosed to unauthorized parties in violation of this understanding. The disclosure occurred because Mr. Cooper failed to implement and maintain reasonable safeguards to protect its customers' PII and failed to comply with industry-standard data security practices.

537. Plaintiffs and Class Members suffered harm the moment an unconsented disclosure of their confidential information to an unauthorized third party occurred.

538. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT VIII
Declaratory and Injunctive Relief

539. Plaintiffs repeat and reallege every allegation in paragraphs 1 through 461.

540. Plaintiffs and the Class pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

541. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal statutes described in this Complaint. An actual controversy has arisen in the wake of the Data Breach regarding Mr. Cooper's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII, and whether Mr. Cooper is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk that further compromises of their PII will occur in the future.

542. The Court should also issue prospective injunctive relief requiring Mr. Cooper to employ adequate security practices consistent with law and industry standards to protect employee and patient PII.

543. Mr. Cooper still possesses the PII of Plaintiffs and the Class.

544. To Plaintiffs' knowledge, Mr. Cooper has made no announcement that it has

changed its data storage or security practices relating to the PII.

545. To Plaintiffs' knowledge, Mr. Cooper has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

546. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Mr. Cooper. The risk of another such breach is real, immediate, and substantial.

547. As described above, actual harm has arisen in the wake of the Data Breach regarding Mr. Cooper's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Mr. Cooper's failure to address the security failings that led to such exposure.

548. There is no reason to believe that Mr. Cooper's employee training and security measures are any more adequate now than they were before the breach to meet Mr. Cooper's contractual obligations and legal duties.

549. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Mr. Cooper if an injunction is issued. Among other things, if another data breach occurs at Mr. Cooper, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Mr. Cooper of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Mr. Cooper has a pre-existing legal obligation to employ such measures.

550. Issuance of the requested injunction will not disserve the public interest. To the

contrary, such an injunction would benefit the public by preventing another data breach at Mr. Cooper, thus eliminating the additional injuries that would result to Plaintiffs and the Class.

551. Plaintiffs and Class Members therefore seek a declaration (1) that Mr. Cooper's existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security, and (2) that to comply with its contractual obligations and duties of care, Mr. Cooper must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Mr. Cooper engage internal security personnel to conduct testing, including audits on Mr. Cooper's systems, on a periodic basis, and ordering Mr. Cooper to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Mr. Cooper engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Mr. Cooper audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Mr. Cooper purge, delete, and destroy, in a reasonably secure manner, any PII not necessary for its provision of services;

e. Ordering that Mr. Cooper conduct regular database scanning and security checks;

f. Ordering that Mr. Cooper routinely and continually conduct internal training

and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information; and

g. Appointing an independent third party assessor, at Defendants' costs, to assess on an annual basis for a period of 10 years Defendants' compliance with the injunctive relief ordered by the Court, as well as to ensure and make recommendations to the Court if Defendants fail to maintain and implement current technology and systems to protect the PII of Plaintiffs and Class Members. The annual report should be filed with the Court under seal and provided to Plaintiffs' counsel to ensure that Defendants cure any deficiencies noted in the annual assessment and make any changes recommended by the independent assessor.

COUNT IX

Violations of the California Consumer Privacy Act
California Civil Code § 1798.150
(On Behalf of Plaintiffs and the California Subclass)

552. Plaintiffs Denver Dale, Chris Lepitak, and Karen Lynn Williams (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 of this Complaint as though fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

553. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . is

subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action" for statutory damages, actual damages, injunctive relief, declaratory relief and any other relief the court deems proper.

554. Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiffs and the California Class. As a direct and proximate result, Plaintiffs' and the California Class's nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

555. Each of Defendants is a "business" under the meaning of Civil Code § 1798.140 because each is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code § 1798.140(d).

556. Plaintiffs and California Class Members are "consumers" as defined by Cal. Civ. Code § 1798.140(g) because they are natural persons who reside in California.

557. Plaintiffs and California Class Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because

Defendants continue to hold Private Information, including Plaintiffs' and Class Members' Private Information.

558. Plaintiffs and California Class Members have an interest in ensuring that their Private Information is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

559. Defendants have long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous related actions against it arising from the Data Breach, the first of which were filed on November 3, 2023 (*Cabezas*). Further, each Defendant is the party with the most knowledge of the underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would not put Defendants in a better position to evaluate those claims. Plaintiffs further sent Defendants notice consistent with the CCPA on or about May 20, 2024, July 2, 2024, and July 8, 2024.

560. Each Defendant failed to take sufficient and reasonable measures to safeguard its data security systems and protect Plaintiffs' and California Class Members' highly sensitive Private Information from unauthorized access. Defendants' failure to maintain adequate data protections subjected Plaintiffs' and the California Class Members' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

561. The unauthorized access, exfiltration, theft, and disclosure of Plaintiffs and the California Subclass Members' Private Information was a result of Defendants' violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information.

562. Under Defendants' duty to protect customers' Private Information, each was

required to implement reasonable security measures to prevent and deter hackers from accessing the Private Information of its customers. These vulnerabilities existed and enabled unauthorized third parties to access and harvest customers' Private Information, evidence that Defendants have breached that duty.

563. Plaintiffs and California Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

564. Defendants' violations of Cal. Civ. Code § 1798.150(a) are a direct and proximate result of the Data Breach.

565. Plaintiffs and California Class Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendants from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

566. Plaintiffs are further entitled to the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

COUNT X

Violations of the California Consumer Records Act Cal. Civ. Code § 1798.80, et seq. ("CCRA") (On Behalf of Plaintiffs and the California Subclass)

567. Plaintiffs Denver Dale, Chris Lepitak, and Karen Lynn Williams (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 as

though fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

568. Plaintiffs bring this claim on behalf of themselves and the California Subclass.

569. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code §1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.*

570. The Data Breach constitutes a "breach of the security system" of Defendants. An unauthorized person acquired the personal, unencrypted information of Plaintiffs and California Subclass Members.

571. Defendants knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the California Class but waited to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

572. Defendants' unreasonable delay prevented Plaintiffs and the California Class from taking appropriate measures from protecting themselves against harm.

573. As a direct or proximate result of Defendants' violations of Civil Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Class Members were (and continue to be)

injured and have suffered (and will continue to suffer) the damages and harms described herein.

574. Plaintiffs accordingly request that the Court enter an injunction requiring Defendants to implement and maintain reasonable security procedures, including, but not limited to: (1) ordering that Defendants utilize strong industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendants, consistent with industry standard practices, engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures; (5) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the

loss of their Private Information.

575. Plaintiffs and California Class Members seek relief under section 1798.84 of the California Civil Code including, but not limited to, actual damages, to be proven at trial, and injunctive relief.

COUNT XI

Violations of the California Unfair Competition Law
California Civil Code § 1798.150
(On Behalf of Plaintiffs and the California Subclass)

576. Plaintiffs Denver Dale, Chris Lepitak, and Karen Lynn Williams (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 as though fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

577. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

578. By reason of Defendants' above-described wrongful actions, inactions, and omissions, the resulting Data Breach, and the unauthorized disclosure of Plaintiffs' and Class Members' Private Information, Defendants engaged in unfair, unlawful, and fraudulent business practices in violation of the UCL.

579. Plaintiffs suffered injury in fact and lost money or property as a result of Defendants' alleged violations of the UCL.

580. The acts, omissions, and conduct of Defendants as alleged herein constitute a "business practice" within the meaning of the UCL.

Unlawful Prong

581. Defendants violated the unlawful prong of the UCL by violating, *inter alia*, the CCPA, CCRA, and GLBA as alleged herein.

582. Defendants violated the unlawful prong of the UCL by failing to honor the terms of its express and implied contracts with Plaintiffs and Class Members, as alleged herein.

583. Defendants' conduct also undermines California public policy—as reflected in the California Information Practices Act, Cal. Civ. Code §§ 1798 et seq., the CCPA concerning consumer privacy, and the CCRA concerning customer records—which seek to protect customer and consumer data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

Unfair Prong

584. Defendants' acts, omissions, and conduct also violate the unfair prong of the UCL because Defendants' acts, omissions, and conduct, as alleged herein, offended public policy and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other Class Members. The gravity of Defendants' conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further Defendants' legitimate business interests, other than Defendants' conduct described herein.

585. Defendants' failure to utilize, and to disclose that it does not utilize, industry standard security practices constitutes an unfair business practice under the UCL. Defendants' conduct is unethical, unscrupulous, and substantially injurious to the Class. While Defendants' competitors have spent the time and money necessary to appropriately safeguard their products,

service, and customer information, Defendants have not—to the detriment of its customers and to competition.

Fraudulent Prong

586. By failing to disclose that it does not enlist industry-standard security practices, all of which rendered Class Members particularly vulnerable to data breaches, each Defendants engaged in UCL-violative practices.

587. A reasonable consumer would not have transacted with Defendants if they knew the truth about their security procedures. By withholding material information about their security practices, Defendants were able to obtain customers who provided and entrusted their Private Information in transacting with Defendants. Had Plaintiffs known the truth about Defendants' security procedures, Plaintiffs would not have patronized Defendants.

588. As a result of Defendants' violations of the UCL, Plaintiffs and Class Members are entitled to injunctive relief including, but not limited to: (1) ordering that Defendants utilize industry standard data security measures for the collection, storage, and retention of customer data; (2) ordering that Defendants, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis; (3) ordering that Defendants engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (4) ordering that Defendants audit, test, and train security personnel regarding any new or modified procedures; (5) ordering that Defendants, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area

of Defendants' systems are compromised, hackers cannot gain access to other portions of those systems; (6) ordering that Defendants purge, delete, and destroy in a reasonably secure manner Class member data not necessary for its provisions of services; (7) ordering that Defendants, consistent with industry standard practices, conduct regular database scanning and security checks; (8) ordering that Defendants, consistent with industry standard practices, evaluate all software, systems, or programs utilized for collection and storage of sensitive Private Information for vulnerabilities to prevent threats to customers; (9) ordering that Defendants, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (10) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their Private Information.

589. As a result of Defendants' violations of the UCL, Plaintiffs and Class Members have suffered injury in fact and lost money or property, as detailed herein. They agreed to transact with Defendants or made purchases or spent money that they otherwise would not have made or spent had they known the true state of affairs regarding Defendants' data security policies. Class Members lost control over their Private Information and suffered a corresponding diminution in value of that Private Information, which is a property right. Class Members lost money as a result of dealing with the fallout of and attempting to mitigate harm arising from the Data Breach.

590. Plaintiffs request that the Court issue sufficient equitable relief to restore Class Members to the position they would have been in had Defendants not engaged in violations of the UCL, including by ordering restitution of all funds that Defendants may have acquired from Plaintiffs and Class Members as a result of those violations. Plaintiffs further allege that their

legal remedies are inadequate.

591. To the extent any of these remedies are equitable, Plaintiffs and Class Members seek such equitable remedies, in the alternative to any adequate remedy at law they may have, including under California's Consumer Privacy Act and California's Consumers Legal Remedies Act.

COUNT XII

Violation of the California Consumer Legal Remedies Act
California Civil Code § 1750, et seq.
(On Behalf of Plaintiffs and the California Subclass)

592. Plaintiffs Denver Dale, Chris Lepitak, and Karen Lynn Williams (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 as though fully set forth herein and bring this claim on behalf of themselves and the California Subclass (the "Class" for the purposes of this count).

593. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq*.

594. Defendants have long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous related actions against it arising from the Data Breach, the first of which were filed on or about November 3, 2023 (*Cabezas*). Further, each Defendant is the party with the most knowledge of the underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would not put Defendants in a better position to evaluate those claims.

595. Plaintiffs further sent Defendants written notice of their violations of the CLRA on or about May 20, 2024, July 2, 2024, and July 8, 2024.

596. Plaintiffs are "consumers," as the term is defined by California Civil Code §

1761(d).

597. Plaintiffs, California Class Members, and Defendants engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

598. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct was undertaken by Defendants was likely to deceive consumers.

599. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

600. Defendants violated this provision by representing that it took appropriate measures to protect Plaintiffs' and California Class Members' Private Information and failing to disclose that its protections were inadequate as alleged herein.

601. Additionally, Defendants improperly handled, stored, or protected either unencrypted or partially encrypted data.

602. As a result, Plaintiffs and California Class Members were induced to enter into a relationship with Defendants and provide their Private Information.

603. Defendants intended to, and did, mislead Plaintiffs and California Class Members and induced them to rely on their omissions.

604. Had Defendants disclosed to Plaintiffs and California Class Members that their data systems were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures

and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and California Class Members' Private Information as part of the services Defendants provided and for which Plaintiffs and California Class Members paid without advising Plaintiffs and California Class Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and California Class Members' Private Information. Accordingly, Plaintiffs and California Class Members acted reasonably in relying on Defendants' omissions, the truth of which they could not have discovered.

605. As a result of engaging in such conduct, Defendants violated Civil Code § 1770.

606. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

607. Plaintiffs and California Class Members suffered injuries caused by Defendants' misrepresentations because they provided their Private Information believing that Defendants would adequately protect this information.

608. Plaintiffs and California Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

609. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiffs and Class Members.

610. Plaintiffs seek prospective injunctive relief, including improvements to Defendants' data security systems and practices, in order to ensure that such security is reasonably sufficient to safeguard customers' Private Information that remains in Defendants' custody, including but not limited to the following:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants not transmit Private Information via unencrypted email;

f. Ordering that Defendants not store Private Information in email accounts;

g. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for provisions of Defendants' services;

h. Ordering that Defendants conduct regular computer system scanning and security checks;

i. Ordering that Defendants routinely and continually conduct internal training

and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendants to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps they must take to protect themselves.

611. Unless such classwide injunctive relief is issued, Plaintiffs and Class Members remain at risk, and there is no other adequate remedy at law that would ensure that Plaintiffs (and other consumers) can rely on Defendants' representations and omissions regarding their data security in the future.

612. To the extent the 30-day cure period has not expired, Plaintiffs seek only injunctive relief pursuant to Cal. Civ. Code § 1782, subdivision (d), which provides that "[a]n action for injunctive relief brought under the specific provisions of Section 1770 may be commenced without compliance with subdivision (a)."

613. To the extent the 30-day cure period under Cal. Civ. Code § 1782(a) has expired, in the alternative to all legal remedies sought herein, Plaintiffs and the Class seek all monetary relief recoverable under the CLRA, including without limitation money damages and restitution; restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices; and attorneys' fees and costs.

COUNT XIII

Violations of the Florida Deceptive and Unfair Trade Practices Act Fla. Stat. § 501.201, et. seq. (On Behalf of Plaintiff and the Florida Subclass)

614. Plaintiff Kay Pollard (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of herself and the Florida Subclass (the "Class" for the purposes of this count).

615. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Defendants obtained Plaintiff's and Class Members' Private Information through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff and Class Members, and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

616. As alleged herein, Defendants engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following:

a. failure to implement adequate data security practices to safeguard Plaintiff's and Class Members' Private Information;

b. failure to make only authorized disclosures of customers' and applicants' Private Information;

c. failure to disclose that their data security practices were inadequate to safeguard customers' Private Information from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiff and Class Members.

617. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and

unscrupulous activities that are and were substantially injurious to Defendants' current and former customers and/or applicants.

618. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices by omitting, failing to disclose, or inadequately disclosing to current and former customers and applicants that they did not follow industry best practices for the collection, use, and storage of Private Information.

619. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class Members are entitled to recover an order providing declaratory relief and reasonable attorneys' fees and costs, to the extent permitted by law.

620. As a direct result of Defendants' knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and Class Members are entitled to injunctive relief, including, but not limited to:

a. ordering that Defendants implement measures that ensure that the Private Information of Defendants' current and former customers and applicants is appropriately encrypted and safeguarded when stored on Defendants' network or systems;

b. ordering that Defendants purge, delete, and destroy in a reasonable secure manner Private Information not necessary for provision of services;

c. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. ordering Defendants to meaningfully educate current and former customers and applicants about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps Defendants' current and former customers must take to protect themselves.

COUNT XIV

Violations of the New York Deceptive Trade Practices Act
New York Gen. Bus. Law § 349
(On Behalf of Plaintiff and the New York Subclass)

621. Plaintiff Gary Allen (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the New York Subclass (for the purposes of this count, the "Class").

622. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;

c. omitting, suppressing, and/or concealing material facts of the inadequacy of its

privacy and security protections for Class Members' Private Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

623. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to them, and that the risk of a data breach or theft was highly likely.

624. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

625. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendants' network and aggregation of Private Information.

626. The representations and omissions upon which Plaintiff and Class Members relied were material (e.g., as to Defendants' adequate protection of Private Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

627. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

628. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York.

629. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

630. As a direct and proximate result of Defendants' multiple, separate violations of GBL § 349, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiffs' and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed Class entrusted Defendants with their Private Information; and (h) the continued and substantial risk to

Plaintiff's and Class Members' Private Information, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' Private Information.

631. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

COUNT XV

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act 815 Ill. Comp. Stat. § 505/1, et seq. (On Behalf of Plaintiffs and the Illinois Subclass)

632. Plaintiffs Jeff Price, Linda Hansen, Izabela Debowczyk, and Larry Siegal (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 as though fully set forth herein and bring this claim on behalf of themselves and the Illinois Subclass (for the purposes of this count, the "Class").

633. Plaintiffs and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Class, and Defendants are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

634. Defendants engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

635. Plaintiffs may bring claims under the ICFA because there is a consumer nexus between Plaintiffs and consumers with respect to Defendants' unfair and deceptive trade practices.

636. Plaintiffs' actions were akin to a consumer's action because they justifiably relied on Defendants' public statements and omissions regarding data security practices. Specifically,

Defendants' statements, including their privacy policy, states Defendants will use reasonable security measures to protect their network from cybercriminals and ransomware attacks.

637. Defendants' representations and omissions as to its data security measures, and failure to implement and maintain reasonable data security measures, concern all individuals because a reasonable consumer, akin to Plaintiffs, does or is reasonably likely to rely on these statements in providing their Private Information.

638. Defendants' conduct involved consumer protection concerns because Defendants represented to consumers and employees (current and former) that they employed proper data security measures but, in fact, did not. Defendants' conduct also involves consumer protection concerns because Defendants' failure to implement and maintain reasonable data security measures enabled third parties to access and exfiltrate the Private Information of consumers from its network. In turn, Plaintiffs' and Class Members' Private Information is now on the dark web.

639. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the ICFA, including: (i) failing to maintain adequate data security to keep Plaintiffs' and the Class Members' sensitive Private Information from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act and GLBA; (ii) failing to disclose or omitting materials facts to Plaintiffs and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiffs and the Class; (iii) failing to disclose or omitting materials facts to Plaintiffs and the Class about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Private Information of

Plaintiffs and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Class's Private Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

640. These actions also constitute deceptive and unfair acts or practices because Defendants knew of their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and the Class and defeat their reasonable expectations about the security of their Private Information.

641. Defendants intended that Plaintiffs and the Class rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of goods and services.

642. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Class. Plaintiffs and the Class have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

643. As a result of Defendants' wrongful conduct, Plaintiffs and the Class were injured in that they never would have provided their Private Information to Defendants, or purchased Defendants' services, had they known or been told that Defendants failed to maintain sufficient security to keep their Private Information from being hacked and taken and misused by others.

644. As a direct and proximate result of Defendants' violations of the ICFA, Plaintiffs and the Class have suffered harm as set forth in detail above.

645. The requested relief by Plaintiffs will assist consumers because it will require Defendants to enhance data security practices. Moreover, any monetary compensation will deter Defendants from additional and future data breach incidents.

646. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs seek actual, compensatory, and punitive damages (815 Ill. Comp. Stat. § 505/10a(c)), injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the ICFA.

COUNT XVI

Violation of the Minnesota Consumer Protection Statute on Deceptive Trade Practices Section 325d.44 and Data Warehouses Section 325E.61 Subdivision 1 (On Behalf of Plaintiff and the Minnesota Subclass)

647. Plaintiff Mychael Marrone (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the Minnesota Subclass (for the purposes of this count, the "Class").

648. The consumer protection statute Minn. R. 325D.44 describes a deceptive trade practice as when in course of business the person "(1) passes off goods or services as those of another;" or "(3) causes likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another;" or "(7) represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another."

649. The consumer protection statute Minn. R. 325E.61 subd. 1 defines "personal information" to inclusive of social security number, driver's license number, and credit card number.

650. Minn. R. 325E.61 subd. 1 also states: "The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system."

651. Defendants advertised, offered, or sold goods or services in Minnesota and engaged in trade or commerce directly or indirectly affecting the people of Minnesota.

652. Defendants represented themselves as providing services compliant with industry standards relating to both mortgage servicing and data security.

653. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Minnesota, including, but not limited to, the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which

was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

654. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

655. Defendants intended to, and did, mislead Plaintiff and Class Members and induced them to rely on their misrepresentations and omissions.

656. Had Defendants disclosed to Plaintiff and Class Members that their data systems

were not secure and, thus, vulnerable to attack, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendants received, maintained, and compiled Plaintiff's and Class Members' Private Information as part of the services Defendants provided and for which Plaintiff and Class Members paid without advising Plaintiff and Class Members that Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Class Members' Private Information. Accordingly, Plaintiff and the Class Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

657. Defendants acted intentionally, knowingly, and maliciously to violate Minnesota law, and recklessly disregarded Plaintiff and Class Members' rights. Defendants were on notice that their security and privacy protections were inadequate and that they were targets of such attacks.

658. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity and cancelling and replacing passports; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

659. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT XVII

Violation of the Colorado Consumer Protection Act
Colo. Rev. Stat. § 6-1-101, et seq.
(On Behalf of Plaintiff and the Colorado Subclass)

660. Plaintiff Elizabeth Curry (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of herself and the Colorado Subclass (for the purposes of this count, the "Class").

661. Defendants engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of services paid for by Plaintiff and Class Members in violation of Colo. Rev. Stat. § 6-1-105, including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which

was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

662. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

663. The above unfair and deceptive practices and acts by Defendants were immoral,

unethical, oppressive, and unscrupulous.

664. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

665. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

666. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

667. Plaintiff and the Class Members seek relief under Colo. Rev. Stat. § 6-1-101 including, but not limited to injunctive relief, compensatory damages, restitution, statutory damages, penalties, and attorneys' fees and costs.

COUNT XVIII

Violation of the North Carolina Unfair Trade Practices Act
N.C. Gen. Stat. An. § 75-1.1, et seq.
(On Behalf of Plaintiff and the North Carolina Subclass)

668. Plaintiff Katy Ross (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of herself and the North Carolina Subclass (for the purposes of this count, the "Class").

669. Defendants' sale, advertising, and marketing of home loan services affected commerce, as meant by N.C. Gen. Stat. § 75-1.1.

670. Defendants engaged in unlawful, unfair, and deceptive acts and practices, with respect to the sale and advertisement of the services paid for by Plaintiff and the Class Members, in violation of N.C. Gen. Stat. § 75-1.1, including by representing that Defendants would adequately protect Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class

Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

671. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

672. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

673. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

674. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

675. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information.

676. Plaintiff and the Class Members seek relief under N.C. Gen. Stat. Ann. §§ 75-16 and 75-16.1, including, but not limited to injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

COUNT XIX

Violation of the Nevada Consumer Fraud Act
Nev Rev. Stat. § 41.600
(On Behalf of Plaintiff and the Nevada Subclass)

677. Plaintiff Brett Padalecki (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 465 as though fully set forth herein and brings this claim on behalf of himself and the Nevada Subclass (for the purposes of this count, the "Class").

678. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600, states: "1. An action may be brought by any person who is a victim of consumer fraud. 2. As used in this section, 'consumer fraud' means: . . . (e) A deceptive trade practice as defined in NRS 598.0915 to 598.0925, inclusive."

679. In turn, Nev. Rev. Stat. § 598.0923(2) (part of the Nevada Deceptive Trade Practices Act) states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 2) Fails to disclose a material fact in connection with the sale or lease of goods or services." Defendants failed to disclose the material

fact that their data security practices were inadequate to reasonably safeguard consumers' Private Information. Defendants knew or should have known that their data security practices were deficient, as explained above. Defendants could and should have made a proper disclosure reasonably calculated to inform consumers of their inadequate data security.

680. Additionally, Nev. Rev. Stat. § 598.0923(3), which is encompassed by the Nevada Consumer Fraud Act quoted above, states: "A person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly: . . . 3) Violates a state or federal statute or regulation relating to the sale or lease of . . . services." Defendants violated this provision.

681. Defendants breached a Nevada statue requiring reasonable data security. Specifically, Nev. Rev. Stat. § 603A.210(1) states: "A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access [or] acquisition." Defendants are data collectors as defined by Nev. Rev. Stat. § 603A.030. Defendants failed to implement and maintain reasonable security measures, evidenced by the Data Breach. Defendants' violation of this statute was done knowingly for purposes of Nev. Rev. Stat. § 598.0923(3) because Defendants knew or should have known that their data security practices were deficient. Defendants also violated the GLBA as explained above.

682. Defendants engaged in deceptive or unfair practices by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

683. Plaintiff and Class Members were denied a benefit conferred on them by the Nevada legislature.

684. Nevada Rev. Stat. § 41.600(3) states that if the plaintiffs prevail, the court "shall award: (a) Any damages that the claimant has sustained; (b) Any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees."

685. As a direct and proximate result of the foregoing, Plaintiff and Class Members suffered all forms of damages alleged herein. Plaintiff's harms constitute compensable damages for purposes of Nev. Rev. Stat. § 41.600(3).

686. Plaintiff and Class Members are also entitled to all forms of injunctive relief sought herein.

687. Plaintiff and Class Members are also entitled to an award of their attorney's fees and costs pursuant to Nev. Rev. Stat. § 41.600(3)(c).

COUNT XX

Violation of the Washington Consumer Protection Act
Wash. Rev. Code Ann. §§ 19.86.020, et seq.
(On Behalf of Plaintiff and the Washington Subclass)

688. Plaintiff Jonathan Josi (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the Washington Subclass (for the purposes of this count, the "Class").

689. Defendants are each a "person" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

690. Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

691. Defendants engaged in unlawful, unfair, and deceptive acts and practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15

U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

692. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

693. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

694. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

695. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

696. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

697. Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislative declaration of public interest impact, and/or injured persons and had the capacity to injure persons. Further, Defendants' conduct affected the public interest, including the Washington victims of the Data Breach.

698. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

COUNT XXI

Violation of the Washington Data Breach Notice Act
Wash. Rev. Code Ann. §§ 19.255.010, et seq.
(On Behalf of Plaintiff and the Washington Subclass)

699. Plaintiff Jonathan Josi (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the Washington Subclass (for the purposes of this count, the "Class").

700. Defendants are each a business that owns or licenses computerized data that includes Private Information as defined by Wash. Rev. Code § 19.255.010(1).

701. Plaintiff's and the Class's Private Information includes information as covered by Wash. Rev. Code § 19.255.010(5).

702. Defendants are required to accurately notify Plaintiff and Washington Class members following discovery or notification of the breach of its data security system if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

703. Because Defendants discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

704. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated Wash. Rev. Code § 19.255.010(1).

705. As a direct and proximate result of Defendants' violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Class members suffered damages, as described above.

706. Plaintiff and Washington Class members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT XXII

Violation of the Louisiana Unfair Trade Practices and Consumer Protection Law La. Rev. Stat. Ann §§ 51:1401, et seq. (On Behalf of Plaintiff and the Louisiana Subclass)

707. Plaintiff Lynette Williams (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings

this claim on behalf of herself and the Louisiana Subclass (for the purposes of this count, the "Class").

708. Defendants are each a "person" as defined by La. Rev. Stat. Ann. § 51:1402(8).

709. Plaintiff and Louisiana Class members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

710. Defendants engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. Ann. § 51:1402(10).

711. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. Stat. Ann. § 51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

712. Defendants engaged in unlawful, unfair, and deceptive acts and practices in the conduct of trade or commerce, including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

713. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them

to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

714. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

715. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

716. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

717. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

718. Plaintiff and Louisiana Class members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Defendants' knowing violations of the Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

COUNT XXIII

Violation of the Louisiana Database Security Breach Notification Law La. Rev. Stat. Ann. §§ 51:3074(A), et seq. (On Behalf of Plaintiff and the Louisiana Subclass)

719. Plaintiff Lynette Williams (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of herself and the Louisiana Subclass (for the purposes of this count, the "Class").

720. Defendants are each a business that owns or licenses computerized data that includes Private Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

721. Plaintiff's and Louisiana Class members' Private Information (e.g., Social Security numbers) includes information as covered by La. Rev. Stat. Ann. § 51:3074(C).

722. Defendants are required to accurately notify Plaintiff and Louisiana Class members following discovery or notification of the breach of its data security system if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

723. Because Defendants discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

724. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated La. Rev. Stat. Ann. § 51:3074(C).

725. As a direct and proximate result of Defendants' violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Class members suffered damages, as described above.

726. Plaintiff and Louisiana Class members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT XXIV

Violation of the Montana Unfair Trade Practices and Consumer Protection Act M.C.A. §§ 30-14-101, et seq.
(On Behalf of Plaintiff and the Montana Subclass)

727. Plaintiff Jose Ignacio Garrigo (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the Montana Subclass (for the purposes of this count, the "Class").

728. Defendants are each a "person" as defined by MCA § 30-14-102(6).

729. Plaintiff and Montana Class members are "consumers" as defined by MCA§ 30-14-102(1).

730. Defendants advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

731. Defendants engaged in unlawful, unfair, and deceptive acts and practices in the conduct of trade or commerce, in violation of MCA § 30-14-103, including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did

not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

732. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

733. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

734. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

735. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

736. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

737. Plaintiff and Montana Class members seek all monetary and non-monetary relief

allowed by law, including the greater of (a) actual damages or (b) statutory damages of $500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

COUNT XXV

Violation of the Montana Computer Security Breach Law
M.C.A. §§ 30-14-1704(1), *et seq*.
(On Behalf of Plaintiff and the Montana Subclass)

738. Plaintiff Jose Ignacio Garrigo (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of himself and the Montana Subclass (for the purposes of this count, the "Class").

739. Defendants are each a business that owns or licenses computerized data that includes Private Information as defined by Mont. Code Ann. § 30-14-1704(4)(b). Defendants also maintain computerized data that includes Private Information which Defendants do not own. Accordingly, Defendants are subject to Mont. Code Ann. § 30-14-1704(1) and (2).

740. Plaintiff's and Montana Class members' Private Information includes information as covered by Mont. Code Ann. § 30-14-1704(4)(b).

741. Defendants are required to give immediate notice of a breach of security of a data system to owners of Private Information which Defendants do not own, including Plaintiff and Montana Class members, pursuant to Mont. Code Ann. § 30-14-1704(2).

742. Defendants are required to accurately notify Plaintiff and Montana Class members if they discover a security breach, or receive notice of a security breach, which may have compromised Private Information which Defendants own or license, without unreasonable delay

under Mont. Code Ann. § 30-14-1704(1).

743. Because Defendants discovered a breach of its security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

744. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

745. As a direct and proximate result of Defendants' violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Class members suffered damages, as described above.

746. Plaintiff and Montana Class members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

COUNT XXVI

Violation of the Missouri Merchandise Practices Act
Mo. Rev. Stat. §§ 407.010, *et seq.*
(On Behalf of Plaintiffs and the Missouri Subclass)

747. Plaintiffs Mary Crawford and Joshua Watson (for purposes of this count, "Plaintiffs") reallege and incorporate by reference paragraphs 1 through 461 as though fully set forth herein and bring this claim on behalf of themselves and the Missouri Subclass (for the purposes of this count, the "Class").

748. Defendants are each a "person" as defined by Mo. Rev. Stat. § 407.010(5).

749. Defendants advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

750. Plaintiff and Missouri Class members purchased or leased goods or services primarily for personal, family, or household purposes.

751. Defendants engaged in unlawful, unfair, and deceptive acts and practices in the conduct of trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality

of Plaintiff and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

752. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

753. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

754. Defendants knew or should have known that their network and data security

practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

755. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

756. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

757. Plaintiff and Missouri Class members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

COUNT XXVII

Violation of the Alabama Deceptive Trade Practices Act
Ala. Code §§ 8-19-1, et seq.
(On Behalf of Plaintiff and the Alabama Subclass)

758. Plaintiff Emily Burke (for purposes of this count, "Plaintiff") realleges and incorporates by reference paragraphs 1 through 461 as though fully set forth herein and brings this claim on behalf of herself and the Alabama Subclass (for the purposes of this count, the "Class").

759. Defendants are each a "person" as defined by Ala. Code § 8-19-3(5).

760. Plaintiff and Alabama Class members are "consumers" as defined by Ala. Code § 8-19-3(2).

761. Defendants advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama.

762. Plaintiff and Missouri Class members purchased or leased goods or services primarily for personal, family, or household purposes.

763. Defendants engaged in unlawful, unfair, and deceptive acts and practices in the conduct of trade or commerce, in violation of Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including by representing that Defendants would safeguard Plaintiff's and the Class Members' Private Information from unauthorized disclosure and release, and comply with relevant state and federal privacy laws, including the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and GLBA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiff and Class Members' Private Information, including by

implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiff and Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

764. Defendants' inadequate data security had no countervailing benefit to consumers or to competition. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on Defendants' misrepresentations and omissions. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

765. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous.

766. Defendants knew or should have known that their network and data security practices were inadequate to safeguard Plaintiff's and the Class Members' Private Information

entrusted to it, and that the risk of a data breach or theft was highly likely.

767. Defendants' actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the Class Members.

768. As a direct and proximate result of Defendants' deceptive acts and practices, Plaintiff and the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

769. Plaintiff and Alabama Class members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and those similarly situated, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their Counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit and prevent Mr. Cooper from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential,

and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Mr. Cooper as a result of their unlawful acts, omissions, and practices;

E. That the Court award to Plaintiffs and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses allowed by law; and

F. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: July 15, 2024

/s/ *Bruce W. Steckler*
Bruce W. Steckler
Texas Bar No. 00785039
STECKLER WAYNE & LOVE, PLLC
12720 Hillcrest Suite 1045
Dallas, TX 75230
Tel: (972) 387-4040
bruce@swclaw.com

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek, Suite 825
Dallas, TX 75219
Tel.: (214) 744-3000
Fax: (877) 744-3728
jkendall@kendalllawgroup.com

Norman E. Siegel* (Missouri Bar No. 44378)
J. Austin Moore* (Missouri Bar No. 64040)
Tanner J. Edwards* (Missouri Bar No 68039)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
tanner@stuevesiegel.com

Gary M. Klinger (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: 866-252-0878
gklinger@milberg.com

John A. Yanchunis
Texas Bar No. 22121300
MORGAN & MORGAN COMPLEX LITIGATION
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Tel: (813) 275-5272
jyanchunis@forthepeople.com

Counsel for Plaintiffs and the Class

** Pro Hac Vice Applications Forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of July 2024, I caused a true and correct copy of the foregoing motion to be filed with the Clerk of the Court for the Northern District of Texas via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

/s/ Bruce W. Steckler
Bruce W. Steckler